

# Improved Inapproximability Results for Counting Independent Sets in the Hard-Core Model

Andreas Galanis\*    Qi Ge†    Daniel Štefankovič†    Eric Vigoda\*    Linji Yang\*

December 12, 2012

## Abstract

We study the computational complexity of approximately counting the number of independent sets of a graph with maximum degree  $\Delta$ . More generally, for an input graph  $G = (V, E)$  and an activity  $\lambda > 0$ , we are interested in the quantity  $Z_G(\lambda)$  defined as the sum over independent sets  $I$  weighted as  $w(I) = \lambda^{|I|}$ . In statistical physics,  $Z_G(\lambda)$  is the partition function for the hard-core model, which is an idealized model of a gas where the particles have non-negligible size. Recently, an interesting phase transition was shown to occur for the complexity of approximating the partition function. Weitz showed an FPAS for the partition function for any graph of maximum degree  $\Delta$  when  $\Delta$  is constant and  $\lambda < \lambda_c(\mathbb{T}_\Delta) := (\Delta - 1)^{\Delta-1}/(\Delta - 2)^\Delta$ . The quantity  $\lambda_c(\mathbb{T}_\Delta)$  is the critical point for the so-called uniqueness threshold on the infinite, regular tree of degree  $\Delta$ . On the other side, Sly proved that there does not exist efficient (randomized) approximation algorithms for  $\lambda_c(\mathbb{T}_\Delta) < \lambda < \lambda_c(\mathbb{T}_\Delta) + \varepsilon(\Delta)$ , unless  $\text{NP}=\text{RP}$ , for some function  $\varepsilon(\Delta) > 0$ . We remove the upper bound in the assumptions of Sly's result for  $\Delta \neq 4, 5$ , that is, we show that there does not exist efficient randomized approximation algorithms for all  $\lambda > \lambda_c(\mathbb{T}_\Delta)$  for  $\Delta = 3$  and  $\Delta \geq 6$ . Sly's inapproximability result uses a clever reduction, combined with a second-moment analysis of Mossel, Weitz and Wormald which prove torpid mixing of the Glauber dynamics for sampling from the associated Gibbs distribution on almost every regular graph of degree  $\Delta$  for the same range of  $\lambda$  as in Sly's result. We extend Sly's result by improving upon the technical work of Mossel et al., via a more detailed analysis of independent sets in random regular graphs.

## 1 Introduction

For a graph  $G = (V, E)$  and activity  $\lambda > 0$ , the hard-core model is defined on the set  $\mathcal{I}(G)$  of independent sets of  $G$  where set  $I \in \mathcal{I}(G)$  has weight  $w(I) := \lambda^{|I|}$ . The so-called partition function for the model is defined as:

$$Z_G(\lambda) := \sum_{I \in \mathcal{I}(G)} w(I) = \sum_{I \in \mathcal{I}(G)} \lambda^{|I|}.$$

The Gibbs distribution  $\mu$  is over the set  $\mathcal{I}(G)$  where  $\mu(I) = w(I)/Z_G(\lambda)$ . The case  $\lambda = 1$  is especially interesting from a combinatorial perspective, since the partition function is the number of independent sets in  $G$  and the Gibbs distribution is uniformly distributed over the set of independent sets.

The hard-core model has received considerable attention in several fields. In statistical physics, it is studied as an idealized model of a gas where the gas particles have non-negligible size so

---

\*School of Computer Science, Georgia Institute of Technology, Atlanta GA 30332. Email: {agalanis,vigoda,ljyang}@cc.gatech.edu. Research supported in part by NSF grant CCF-0830298 and CCF-0910584.

†Department of Computer Science, University of Rochester, Rochester, NY 14627. Email: {qge,stefanko}@cs.rochester.edu. Research supported in part by NSF grant CCF-0910415.

neighboring sites cannot simultaneously be occupied [3, 1]. The activity  $\lambda$  corresponds to the fugacity of the gas. The model also arose in operations research in the study of communication networks [7].

We study the computational complexity of approximating the partition function. Valiant [15] proved that exactly computing the number of independent sets of an input graph  $G = (V, E)$  is #P-complete. Greenhill [4] proved that even when the input is restricted to graphs with maximum degree 3, it is still #P-complete. Hence, our focus is on approximating the partition function.

Weitz [16] gave an FPAS (fully polynomial-time approximation scheme) for the partition function of graphs with maximum degree  $\Delta$  when  $\Delta$  is constant and  $\lambda < \lambda_c(\mathbb{T}_\Delta) := (\Delta-1)^{\Delta-1}/(\Delta-2)^\Delta$ . The activity  $\lambda_c(\mathbb{T}_\Delta)$  is the critical activity for the threshold of uniqueness/non-uniqueness of the infinite-volume Gibbs measures on the infinite  $\Delta$ -regular tree [7]. Recently, Sly [11] proved that, unless  $NP = RP$ , for every  $\Delta \geq 3$ , there exists a function  $\varepsilon(\Delta) > 0$  such that for graphs with maximum degree  $\Delta$  there does not exist an FPRAS (fully-polynomial time randomized approximation scheme) for the partition function at activity  $\lambda$  satisfying:

$$\lambda_c(\mathbb{T}_\Delta) < \lambda < \lambda_c(\mathbb{T}_\Delta) + \varepsilon(\Delta). \quad (\star)$$

It was conjectured in Sly [11] and Mossel et al. [10] that the inapproximability result holds for all  $\lambda > \lambda_c(\mathbb{T}_\Delta)$ . We almost resolve this conjecture, that is we prove the conjecture for all  $\Delta$  with the exception of  $\Delta \in \{4, 5\}$ .

**Theorem 1.** *Unless  $NP=RP$ , there does not exist an FPRAS for the partition function of the hard-core model for graphs of maximum degree at most  $\Delta$  at activity  $\lambda$  when:*

- $\Delta = 3$  and  $\lambda > \lambda_c(\mathbb{T}_3) = 4$ ; or
- $\Delta \geq 6$  and  $\lambda > \lambda_c(\mathbb{T}_\Delta)$ ; or
- $\Delta = 4$  and  $\lambda \in (\lambda_c(\mathbb{T}_4) = 1.6875, 2.01538] \cup (4, +\infty)$ ; or
- $\Delta = 5$  and  $\lambda \in (\lambda_c(\mathbb{T}_5) = 256/243, 1.45641] \cup (1.6875, 2.01538] \cup (4, +\infty)$ .

Sly's work utilizes earlier work of Mossel et al. [10] which studied the Glauber dynamics. The Glauber dynamics is a simple Markov chain  $(X_t)$  that is used to sample from the Gibbs distribution (and hence to approximate the partition function via now standard techniques, see [6, 12]). For an input graph  $G = (V, E)$  and activity  $\lambda > 0$ , the state space of the chain is  $\mathcal{I}(G)$ . From a state  $X_t \in \mathcal{I}(G)$ , the transitions  $X_t \rightarrow X_{t+1}$  are defined by the following stochastic process:

- Choose a vertex  $v$  uniformly at random from  $V$ .
- Let

$$X' = \begin{cases} X_t \cup \{v\} & \text{with probability } \lambda/(1+\lambda) \\ X_t \setminus \{v\} & \text{with probability } 1/(1+\lambda). \end{cases}$$

- If  $X' \in \mathcal{I}(G)$ , then set  $X_{t+1} = X'$ , otherwise set  $X_{t+1} = X_t$ .

It is straightforward to verify that the Glauber dynamics is ergodic, and the unique stationary distribution is the Gibbs distribution. The mixing time  $T_{\text{mix}}$  is the minimum number of steps  $T$  from the worst initial state  $X_0$ , so that the distribution of  $X_T$  is within (total) variation distance  $\leq 1/4$  of the stationary distribution. The chain is said to be *rapidly mixing* if the mixing time is polynomial in  $n = |V|$ , and it is said to be *torpidly mixing* if the mixing time is exponential in  $n$ .

(for the purposes of this paper, that means  $T_{\text{mix}} = \exp(\Omega(n))$ ). We refer the reader to Levin et al. [8] for a more thorough introduction to the Glauber dynamics.

Mossel et al. [10] proved that the Glauber dynamics is torpidly mixing, for all  $\Delta \geq 3$ , for graphs with maximum degree  $\Delta$  when  $\lambda$  satisfies  $(\star)$ . This result improved upon earlier work of Dyer et al. [2] which held for larger  $\lambda$ , but not down to the critical activity  $\lambda_c(\mathbb{T}_\Delta)$ . The torpid mixing result of Mossel et al. [10] follows immediately (via a conductance argument) from their main result that for a random  $\Delta$ -regular bipartite graph, for  $\lambda$  satisfying  $(\star)$ , an independent set drawn from the Gibbs distribution is “unbalanced” with high probability.

The proof of Mossel et al. [10] is a technically involved second moment calculation that Sly [11] calls a “technical tour de force”. Our main contribution is to improve upon Mossel et al.’s result, most notably, extending it to all  $\lambda > \lambda_c(\mathbb{T}_\Delta)$  for  $\Delta = 3$ . Our improved analysis comes from using a slightly different parameterization of the second moment of the partition function, which brings in symmetry, and allows for simpler proofs.

To formally state our results for independent sets of random regular graphs, we need to partition the set of independent sets as follows. For a bipartite graph  $G = (V_1 \cup V_2, E)$  where  $|V_1| = |V_2| = n$ , for  $\delta > 0$ , for  $i \in \{1, 2\}$ , let

$$\mathcal{I}_i^\delta = \{I \in \mathcal{I}(G) : |I \cap V_i| > |I \cap V_{3-i}| + \delta n\}$$

denote the independent sets that are unbalanced and “biased” towards  $V_i$ . Let

$$\mathcal{I}_B^\delta = \{I \in \mathcal{I}(G) : |I \cap V_i| \leq |I \cap V_{3-i}| + \delta n\}$$

denote the set of nearly balanced independent sets.

Let  $\mathcal{G}(n, \Delta)$  denote the probability distribution over bipartite graphs with  $n + n$  vertices formed by taking the union of  $\Delta$  random perfect matchings. Strictly speaking, this distribution is over multi-graphs. However, for independent sets the multiplicity of an edge does not matter so we can view  $\mathcal{G}(n, \Delta)$  as a distribution over simple graphs with maximum degree  $\Delta$ . Moreover, since our results hold asymptotically almost surely (a.a.s.) over  $\mathcal{G}(n, \Delta)$ , as noted in [10, Section 2.1], by standard arguments (see the note after the proof of [9, Theorem 4]), our results also hold a.a.s. for the uniform distribution over bipartite  $\Delta$ -regular graphs.

**Theorem 2.** *For  $\Delta = 3$  and any  $\lambda > \lambda_c(\mathbb{T}_\Delta)$ , there exist  $a > 1$  and  $\delta > 0$  such that, asymptotically almost surely, for a graph  $G$  chosen from  $\mathcal{G}(n, \Delta)$ , the Gibbs distribution  $\mu$  satisfies:*

$$\mu(\mathcal{I}_B^\delta) \leq a^{-n} \min\{\mu(\mathcal{I}_1^\delta), \mu(\mathcal{I}_2^\delta)\}.$$

*Therefore, the Glauber dynamics is torpidly mixing.*

This proves Conjecture 2.4 of [10] for the case  $d = 3$ . For  $\Delta \geq 4$  we can extend Mossel et al.’s results to a larger range of  $\lambda$  than previously known.

**Theorem 3.** *For all  $\Delta \geq 4$  there exists  $\varepsilon(\Delta) > 0$ , for any  $\lambda$  where  $\lambda_c(\mathbb{T}_\Delta) < \lambda < \lambda_c(\mathbb{T}_\Delta) + \varepsilon(\Delta)$ , there exist  $a > 1$  and  $\delta > 0$  such that, asymptotically almost surely, for a graph  $G$  chosen from  $\mathcal{G}(n, \Delta)$ , the Gibbs distribution  $\mu$  satisfies:*

$$\mu(\mathcal{I}_B^\delta) \leq a^{-n} \min\{\mu(\mathcal{I}_1^\delta), \mu(\mathcal{I}_2^\delta)\}.$$

*Therefore, the Glauber dynamics is torpidly mixing. The function  $\varepsilon(\Delta)$  satisfies:*

- If  $\Delta \geq 6$ ,  $\varepsilon(\Delta) \geq \lambda_c(\mathbb{T}_\Delta) - \lambda_c(\mathbb{T}_{\Delta+1})$ .

- For  $\Delta = 5$ ,  $\varepsilon(5) \geq .402912$ .
- For  $\Delta = 4$ ,  $\varepsilon(4) \geq .327887$ .

In the following section we look at the first and second moments of the partition function. We then state two technical lemmas (Lemma 10 and Lemma 11) from which Theorems 1, 2 and 3 easily follow using work of Sly [11] and Mossel et al. [10]. In Section 4 we prove the technical lemmas. Some of our proofs use Mathematica to prove inequalities involving rational functions, this is discussed in Section 2.5.

## 2 Overview

Proceeding as in [10] and [11], roughly speaking, to prove Theorems 1, 2 and 3 we need to prove that there exist graphs  $G$  whose partition function is close to the expected value (where the expectation is over a random  $G \sim \mathcal{G}(n, \Delta)$ ). At the heart of the argument lies a careful analysis of the first two moments of the partition function. The aim of this Section is to give a brief technical overview of the analysis. For more details, the reader is referred to [10] and [11].

In Section 2.1, we define the quantities which will be prevalent throughout the text. In Sections 2.2 and 2.3, we revisit the first and second moments and state our main technical Lemma. We then prove Theorems 1, 2 and 3 in Section 2.4. In Section 2.5, we clarify our use of computer assistance for the proofs of some technical inequalities.

### 2.1 Phase Transition Revisited

Recall, for the infinite  $\Delta$ -regular tree  $\mathbb{T}_\Delta$ , Kelly [7] showed that there is a phase transition at  $\lambda_c(\mathbb{T}_\Delta) = (\Delta - 1)^{\Delta-1}/(\Delta - 2)^\Delta$ . Formally, this phase transition can be defined in the following manner. Let  $T_\ell$  denote the complete tree of degree  $\Delta$  and containing  $\ell$  levels. Let  $p_\ell$  denote the marginal probability that the root is occupied in the Gibbs distribution on  $T_\ell$ . Note, for even  $\ell$  the root is in the maximum independent set, whereas for odd  $\ell$  the root is not in the maximum independent set. Our interest is in comparing the marginal probability for the root in even versus odd sized trees. Hence, let

$$p^+ = \lim_{\ell \rightarrow \infty} p_{2\ell} \quad \text{and} \quad p^- = \lim_{\ell \rightarrow \infty} p_{2\ell+1}.$$

One can prove these limits exist by analyzing appropriate recurrences. The phase transition on the tree  $\mathbb{T}_\Delta$  captures whether  $p^+$  equals (or not)  $p^-$ . For all  $\lambda \leq \lambda_c(\mathbb{T}_\Delta)$ , we have  $p^+ = p^-$ , and let  $p^* := p^+ = p^-$ . On the other side, for all  $\lambda > \lambda_c(\mathbb{T}_\Delta)$ , we have  $p^+ > p^-$ . Mossel et al. [10] exhibited the critical role these quantities  $p^+$  and  $p^-$  play in the analysis of the Gibbs distribution on random graphs  $\mathcal{G}(n, \Delta)$ .

### 2.2 First Moment of the Partition Function

Let  $G \sim \mathcal{G}(n, \Delta)$ . For  $\alpha, \beta \geq 0$ , let

$$\mathcal{I}_G^{\alpha, \beta} = \{I \in \mathcal{I}_G \mid |I \cap V_1| = \alpha n, |I \cap V_2| = \beta n\},$$

that is,  $\alpha$  is the fraction of the vertices in  $V_1$  that are in the independent set and  $\beta$  is the fraction of the vertices in  $V_2$  for an independent set of a bipartite graph  $G$ . We consider only values of  $(\alpha, \beta)$  in the region

$$\mathcal{R} = \{(\alpha, \beta) \mid \alpha, \beta \geq 0 \text{ and } \alpha + \beta \leq 1\},$$

since it is straightforward to see that for a graph  $G \sim \mathcal{G}(n, \Delta)$ , it *deterministically* holds that  $\mathcal{I}_G^{\alpha, \beta} = \emptyset$  whenever  $(\alpha, \beta) \notin \mathcal{R}$ . For  $(\alpha, \beta) \in \mathcal{R}$ , define also

$$Z_G^{\alpha, \beta} = \sum_{I \in \mathcal{I}_G^{\alpha, \beta}} \lambda^{(\alpha + \beta)n},$$

i.e.,  $Z_G^{\alpha, \beta}$  is the total weight of independent sets in  $\mathcal{I}_G^{\alpha, \beta}$ . The first moment of  $Z_G^{\alpha, \beta}$  is

$$\mathbb{E}_{\mathcal{G}}[Z_G^{\alpha, \beta}] = \lambda^{(\alpha + \beta)n} \binom{n}{\alpha n} \binom{n}{\beta n} \left( \frac{\binom{(1 - \beta)n}{\alpha n}}{\binom{n}{\alpha n}} \right)^{\Delta} \approx \exp(n \Phi_1(\alpha, \beta)),$$

where

$$\Phi_1(\alpha, \beta) = (\alpha + \beta) \ln(\lambda) + H(\alpha) + H(\beta) + \Delta(1 - \beta)H\left(\frac{\alpha}{1 - \beta}\right) - \Delta H(\alpha),$$

and  $H(x) = -x \ln x - (1 - x) \ln(1 - x)$  is the entropy function. The asymptotic order of  $\mathbb{E}_{\mathcal{G}}[Z_G^{\alpha, \beta}]$  follows easily by Stirling's approximation.

The first moment was analyzed in the work of Dyer et al. [2]. We use the following lemma from Mossel et al. [10] that relates the properties of the first moment to  $p^*, p^+$  and  $p^-$ . The most important aspect of this lemma is that in the non-uniqueness region  $\mathbb{E}_{\mathcal{G}}[Z_G^{\alpha, \beta}]$  is maximized when  $\alpha \neq \beta$  ([2]) and more specifically for  $(\alpha, \beta) = (p^+, p^-)$  ([10]).

**Lemma 4** (Lemma 3.2 and Proposition 4.1 of Mossel et al. [10]). *The following holds:*

1. *the stationary point  $(\alpha, \beta)$  of  $\Phi_1$  over  $\mathcal{R}$  is the solution to  $\beta = \phi(\alpha)$  and  $\alpha = \phi(\beta)$ , where*

$$\phi(x) = (1 - x) \left( 1 - \left( \frac{x}{\lambda(1 - x)} \right)^{1/\Delta} \right), \quad (1)$$

*and the solutions are exactly  $(p^+, p^-)$ ,  $(p^-, p^+)$ , and  $(p^*, p^*)$  when  $\lambda > \lambda_c(\mathbb{T}_{\Delta})$ , and the unique solution is  $(p^*, p^*)$  when  $\lambda \leq \lambda_c(\mathbb{T}_{\Delta})$ ;*

2. *when  $\lambda \leq \lambda_c(\mathbb{T}_{\Delta})$ ,  $(p^*, p^*)$  is the unique maximum of  $\Phi_1$  over  $\mathcal{R}$ , and when  $\lambda > \lambda_c(\mathbb{T}_{\Delta})$ ,  $(p^+, p^-)$  and  $(p^-, p^+)$  are the maxima of  $\Phi_1$  over  $\mathcal{R}$ , and  $(p^*, p^*)$  is not a local maximum;*
3. *all local maxima of  $\Phi_1$  satisfy  $\alpha + \beta + \Delta(\Delta - 2)\alpha\beta \leq 1$ ;*
4.  *$p^+, p^-, p^*$  satisfy  $p^- < p^* < p^+$  and when  $\lambda \rightarrow \lambda_c(\mathbb{T}_{\Delta})$  from above, we have  $p^*, p^-, p^+ \rightarrow 1/\Delta$ .*

For every  $\Delta \geq 3$ , define the region

$$\mathcal{R}_{\Delta} = \{(\alpha, \beta) \mid \alpha, \beta > 0 \text{ and } \alpha + \beta + \Delta(\Delta - 2)\alpha\beta \leq 1\}.$$

Part 3 of Lemma 4 establishes that the local maxima of  $\Phi_1$  lie in  $\mathcal{R}_{\Delta}$ . Note that for  $\Delta \geq 3$ , we have  $\mathcal{R}_{\Delta} \subset \mathcal{R}$ . Hence, the local maxima for all  $\Delta \geq 3$  lie in the interior of  $\mathcal{R}$ .

## 2.3 Second Moment of the Partition Function

The second moment of  $Z_G^{\alpha, \beta}$  satisfies ([10])

$$\mathbb{E}_{\mathcal{G}}[(Z_G^{\alpha, \beta})^2] \approx \exp(n \cdot \max_{\gamma, \delta, \varepsilon} \Phi_2(\alpha, \beta, \gamma, \delta, \varepsilon)),$$

where

$$\begin{aligned}\Phi_2(\alpha, \beta, \gamma, \delta, \varepsilon) = & 2(\alpha + \beta) \ln(\lambda) + H(\alpha) + H_1(\gamma, \alpha) + H_1(\alpha - \gamma, 1 - \alpha) + H(\beta) + H_1(\delta, \beta) \\ & + H_1(\beta - \delta, 1 - \beta) + \Delta \left( H_1(\gamma, 1 - 2\beta + \delta) - H(\gamma) + H_1(\varepsilon, 1 - 2\beta + \delta - \gamma) \right. \\ & + H_1(\alpha - \gamma - \varepsilon, \beta - \delta) - H_1(\alpha - \gamma, 1 - \gamma) + H_1(\alpha - \gamma, 1 - \beta - \gamma - \varepsilon) \\ & \left. - H_1(\alpha - \gamma, 1 - \alpha) \right),\end{aligned}\quad (2)$$

and  $H(x) = -x \ln(x) - (1 - x) \ln(1 - x)$ ,  $H_1(x, y) = -x(\ln(x) - \ln(y)) + (x - y)(\ln(y - x) - \ln(y))$ .

To make  $\Phi_2$  well defined, the variables have to satisfy  $(\alpha, \beta) \in \mathcal{R}$  and

$$\begin{aligned}\gamma, \delta, \varepsilon \geq 0, \quad \alpha - \gamma - \varepsilon \geq 0, \quad \beta - \delta \geq 0, \quad 1 - 2\beta + \delta - \gamma - \varepsilon \geq 0, \\ 1 - \alpha - \beta - \varepsilon \geq 0, \quad \beta - \delta + \varepsilon + \gamma - \alpha \geq 0.\end{aligned}\quad (3)$$

Lemma 4 tells us that in the non-uniqueness region (which is the region of interest in this paper) the first moment is maximized when  $(\alpha, \beta)$  is  $(p^+, p^-)$  (or symmetrically,  $(p^-, p^+)$ ). To show that these unbiased configurations dominate the Gibbs distribution with high probability (as desired for Theorems 2 and 3 we will apply the second moment method, as used in [10].

To that end, we need to analyze the second moment for  $(\alpha, \beta) = (p^+, p^-)$ , and show that  $\mathbb{E}_{\mathcal{G}}[(Z_G^{\alpha, \beta})^2] = O((\mathbb{E}_{\mathcal{G}}[Z_G^{\alpha, \beta}])^2)$ . To do that we need to show that for  $(\alpha, \beta) = (p^+, p^-)$ ,  $\mathbb{E}_{\mathcal{G}}[(Z_G^{\alpha, \beta})^2]$  is roughly determined by uncorrelated pairs of configurations. This crux of this is to show that  $\Phi_2$  is maximized when  $\gamma = \alpha^2$  and  $\delta = \beta^2$ , which is detailed in the upcoming condition which was proposed in [11].

**Condition 1** (Condition 1.2<sup>1</sup> of Sly [11]). *There exists a constant  $\chi > 0$  such that when  $|p^+ - \alpha| < \chi$  and  $|p^- - \beta| < \chi$  then  $g_{\alpha, \beta}(\gamma, \delta, \varepsilon) := \Phi_2(\alpha, \beta, \gamma, \delta, \varepsilon)$  achieves its unique maximum in the region (3) at the point*

$$(\gamma^*, \delta^*, \varepsilon^*) = (\alpha^2, \beta^2, \alpha(1 - \alpha - \beta)).$$

As mentioned earlier, Condition 1 implies that for  $(\alpha, \beta) = (p^+, p^-)$ ,  $\mathbb{E}_{\mathcal{G}}[(Z_G^{\alpha, \beta})^2] = O((\mathbb{E}_{\mathcal{G}}[Z_G^{\alpha, \beta}])^2)$ . While the implicit constant in the latter equality is bigger than one, an application of the small graph conditioning method [5, 17] shows that for  $(\alpha, \beta) = (p^+, p^-)$ ,  $Z_G^{\alpha, \beta}$  is concentrated around its expected value (up to a multiplicative arbitrarily small polynomial factor). This yields a lower bound on the partition function  $Z_G^{\alpha, \beta}$  for  $(\alpha, \beta) = (p^+, p^-)$ . On the other hand, it is straightforward to an upper bound on the partition function for balanced configurations  $\alpha = \beta$ . Consequently, one obtains Theorems 2 and 3 as detailed below in Section 2.4, which implies that the Gibbs distribution is unbalanced with high probability. Sly [11] uses random regular bipartite graphs as a gadget in his reduction and utilizes this bimodality property of the Gibbs distribution.

Before stating our new results on when Condition 1 holds, it is useful to remind the reader the previously known values of  $\lambda$  for which Condition 1 holds:

- $\Delta \geq 3$ , and  $\lambda_c(\mathbb{T}_\Delta) < \lambda < \lambda_c(\mathbb{T}_\Delta) + \varepsilon(\Delta)$  for some (small)  $\varepsilon(\Delta) > 0$ , ([10, Lemma 6.10, Lemma 5.1]);
- $\Delta = 6$  and  $\lambda = 1$ , ([11, Section 5]).

Let  $\lambda_{1/2}(\mathbb{T}_\Delta)$  be the smallest value of  $\lambda$  such that  $\phi(\phi(1/2)) = 1/2$  ( $\phi$  is the function defined in Lemma 4). Equivalently  $\lambda_{1/2}(\mathbb{T}_\Delta)$  is the minimum solution of

$$\left(1 + (1/\lambda)^{1/\Delta}\right)^{1-1/\Delta} \left(1 - (1/\lambda)^{1/\Delta}\right)^{1/\Delta} = 1. \quad (4)$$

---

<sup>1</sup>The numbering in this paper for results from Sly's work [11] refer to the **arXiv** version of his paper.

The following Lemma is the technical core of this work.

**Lemma 5.** *Condition 1 holds for*

1.  $\Delta = 3$  and  $\lambda > \lambda_c(\mathbb{T}_\Delta)$ , and
2.  $\Delta > 3$  and  $\lambda \in (\lambda_c(\mathbb{T}_\Delta), \lambda_{1/2}(\mathbb{T}_\Delta)]$ ,

Lemma 5 is proved in Section 4. As a corollary of Lemma 5 we get that Condition 1 holds for the range of  $\lambda$  specified in Theorems 2 and 3.

**Corollary 6.** *Condition 1 holds for:*

1. For  $\Delta = 3$  and  $\lambda > \lambda_c(\mathbb{T}_3)$ .
2. For  $\Delta \geq 6$  and  $\lambda_c(\mathbb{T}_\Delta) < \lambda \leq \lambda_{1/2}(\mathbb{T}_\Delta)$  and  $\lambda_{1/2}(\mathbb{T}_\Delta) > \lambda_c(\mathbb{T}_{\Delta-1})$ .
3. For  $\Delta = 5$  and  $\lambda_c(\mathbb{T}_5) < \lambda \leq \lambda_c(\mathbb{T}_5) + .402912$ .
4. For  $\Delta = 4$ ,  $\lambda_c(\mathbb{T}_4) < \lambda \leq \lambda_c(\mathbb{T}_4) + .327887$ .

*Proof.* Part 1 is identical to the first bullet in Lemma 5.

Part 2 follows from the second bullet of Lemma 5 and the fact that for  $\Delta \geq 6$ , it holds  $\lambda_{1/2}(\mathbb{T}_\Delta) > \lambda_c(\mathbb{T}_{\Delta-1})$ . To see this, by (4), we have that  $1 - (1/\lambda_{1/2}(\mathbb{T}_\Delta))^{1/\Delta} > 0$ , which implies that  $\lambda_{1/2}(\mathbb{T}_\Delta) > 1$ . For  $\Delta \geq 6$ , we have  $\lambda_c(\mathbb{T}_\Delta) < 1$ . Hence, for  $\Delta \geq 7$ , we have  $\lambda_{1/2}(\mathbb{T}_\Delta) > \lambda_c(\mathbb{T}_{\Delta-1})$ . For  $\Delta = 6$ , the claim follows from the fact that  $\lambda_c(\mathbb{T}_5) = 256/243 < \lambda_{1/2}(\mathbb{T}_6) \approx 1.23105$ .

For  $\Delta = 5$ , note that

$$\lambda_{1/2}(\mathbb{T}_5) - \lambda_c(\mathbb{T}_5) > 1.45641 - 256/243 > .402912,$$

which proves Part 3.

For  $\Delta = 4$ , note that

$$\lambda_{1/2}(\mathbb{T}_4) - \lambda_c(\mathbb{T}_4) > 2.015387 - 27/16 = .327887,$$

which proves Part 4. □

Theorems 2 and 3 now follow from Corollary 6 as outlined earlier, and detailed in the following subsection.

## 2.4 Proofs of Main Theorems

We now proceed to prove Theorems 2 and 3.

*Proofs of Theorems 2 and 3.* The proof is essentially the same as the proof of [10, Theorem 2.2] with minor modifications. We include the proof for the sake of completeness.

Choose  $\delta > 0$  such that for

$$X := \min_{|x-p^+| \leq \delta, |y-p^-| \leq \delta} \Phi_1(x, y), \quad Y := \max_{|x-y| \leq \delta} \Phi_1(x, y)$$

it holds that  $\tau := X - Y > 0$ . To see that this is possible, note that  $\Phi_1$  is continuous and hence it is uniformly continuous at any closed and bounded region. Since  $\Phi_1$  exhibits a global maximum at  $(p^+, p^-)$ , the existence of  $\delta$  follows.



By Markov's inequality, we obtain that a.a.s.

$$\mu(\mathcal{I}_B^\delta) = \frac{\sum_{x,y:|x-y|\leq\delta} Z_G^{x,y}}{Z_G} \leq \frac{\exp(n(Y + \frac{\tau}{4}))}{Z_G}. \quad (5)$$

To bound  $\min\{\mu(\mathcal{I}_1^\delta), \mu(\mathcal{I}_2^\delta)\}$ , we need the following result from [10]. While their result is only stated for  $(\alpha, \beta)$  close to  $(1/\Delta, 1/\Delta)$ , it can readily be verified (as Sly also observed, e.g., see the discussion before Lemma 3.4 in [11]) that their proof holds in a neighbourhood of  $(p^+, p^-)$ , whenever Condition 1 holds.

**Lemma 7** (Theorem 3.4 of Mossel et al. [10]). <sup>2</sup> *Let  $\Delta \geq 3$ . Suppose that Condition 1 holds, then for all sufficiently large  $n$  there exist  $(\alpha_n, \beta_n)$  where*

$$\alpha_n = p^+ + o(1), \quad \beta_n = p^- + o(1), \quad \text{and } n\alpha_n \text{ and } n\beta_n \text{ are integers}, \quad (6)$$

and it holds a.a.s. that

$$Z_G^{\alpha_n, \beta_n} \geq \frac{1}{n} \mathbb{E}_{\mathcal{G}}[Z_G^{\alpha_n, \beta_n}].$$

For all  $n$  large enough, there exist  $(\alpha_n, \beta_n)$  where  $|\alpha_n - p^+| \leq 1/n$ ,  $|\beta_n - p^-| \leq 1/n$  and  $n\alpha_n$  and  $n\beta_n$  are integers, and therefore (6) holds.

From Lemma 7 and Corollary 6 it follows that a.a.s.  $Z_G^{\alpha, \beta} \geq \exp(n(X - \frac{\tau}{4}))$  and consequently

$$\mu(\mathcal{I}_1^\delta) \geq \frac{\exp(n(X - \frac{\tau}{4}))}{Z_G}.$$

Since both  $\Phi_1$  and  $\Phi_2$  are symmetric with respect to  $\alpha, \beta$ , a similar statement to Lemma 7 holds with the roles of  $p^+, p^-$  interchanged, so that

$$\min\{\mu(\mathcal{I}_1^\delta), \mu(\mathcal{I}_2^\delta)\} \geq \frac{\exp(n(X - \frac{\tau}{4}))}{Z_G}. \quad (7)$$

Combining (5) and (7), we obtain

$$\mu(\mathcal{I}_B^\delta) \leq \exp(-\frac{n\tau}{2}) \min\{\mu(\mathcal{I}_1^\delta), \mu(\mathcal{I}_2^\delta)\}. \quad (8)$$

This completes the proof.

The torpid mixing of the Glauber dynamics claimed in Theorems 2 and 3 follows from (8) by Claim 2.3 in [2], which is a standard conductance argument.  $\square$

For Theorem 1, we will use Lemma 5 combined with the work of Sly [11], but we need one additional ingredient. The following combinatorial result will be used to extend the inapproximability result for  $\Delta = 3$  to a range of  $\lambda$  for  $\Delta \geq 6$ .

**Lemma 8.** *Let  $G$  be a graph of maximum degree  $\Delta$  and let  $k > 1$  be an integer. Consider the graph  $H$  obtained from  $G$  by replacing each vertex by  $k$  copies of that vertex and each edge by the complete bipartite graph between the corresponding copies. Then,*

$$Z_G((1 + \lambda)^k - 1) = Z_H(\lambda).$$

---

<sup>2</sup>The stated version of the theorem differs slightly from the version in [10]. In particular, in [10]  $(\alpha, \beta)$  is fixed, in the sense that it's independent of  $n$ . Here,  $(\alpha, \beta)$  depends on  $n$ . In the application of this theorem in the proof of Theorem 2.2 in [10], it is unclear how they deduce the existence of a fixed  $(\alpha, \beta)$  and this is why we modified the statement of the theorem. Their proof of Theorem 3.4 in [10] still goes through for this slightly modified version.



*Proof.* Consider the map  $f : \mathcal{I}_H \rightarrow \mathcal{I}_G$  that maps an independent set  $I$  of  $H$  to an independent set  $J$  of  $G$  such that  $v \in J$  if and only if at least one of the  $k$  copies of  $v$  in  $H$  are in  $I$ .

For an independent set  $J$  of  $G$  the total contribution of sets in  $f^{-1}(J)$  to  $Z_H(\lambda)$  is  $((1+\lambda)^k - 1)^{|J|}$ , since for each  $v \in J$  we can choose any non-empty subset of its  $k$  copies in  $H$ .  $\square$

We are now ready to prove Theorem 1.

*Proof of Theorem 1.* Sly's reduction [11, Section 2] establishes that for any  $\lambda > \lambda_c(\mathbb{T}_\Delta)$  such that Condition 1 holds and also the following two inequalities hold:

$$(\Delta - 1)p^+p^- \leq (1 - p^+)(1 - p^-) \text{ and } p^+ < \frac{3}{5}(1 - p^-), \quad (9)$$

then there does not exist (assuming  $\text{NP} \neq \text{RP}$ ) an FPRAS for the partition function of the hard-core model with activity  $\lambda$ . For the two inequalities in (9), as Sly [11] points out, they are unnecessary. First off, the inequality  $(\Delta - 1)p^+p^- \leq (1 - p^+)(1 - p^-)$  is implied by Part 3 of Lemma 4. And the condition  $p^+ < \frac{3}{5}(1 - p^-)$  is used to simplify the proof of Lemma 4.2 in [11]. For completeness, a slight modification of Sly's Lemma 4.2 without (9) in the hypothesis is proved in Section 3.

Corollary 6 establishes that Condition 1 holds for a range of activities  $\lambda$  for each  $\Delta \geq 3$ . By the discussion above, we obtain that there does not exist (assuming  $\text{NP} \neq \text{RP}$ ) an FPRAS for the partition function of the hard-core model with activity

- $\lambda \in (\lambda_c(\mathbb{T}_3), \infty]$  for  $\Delta = 3$ .
- $\lambda \in (\lambda_c(\mathbb{T}_\Delta), \lambda_c(\mathbb{T}_{\Delta-1})]$  for  $\Delta \geq 6$ .
- $\lambda \in (\lambda_c(\mathbb{T}_5), \lambda_c(\mathbb{T}_5) + .402912]$  for  $\Delta = 5$ .
- $\lambda \in (\lambda_c(\mathbb{T}_4), \lambda_c(\mathbb{T}_4) + .327887]$  for  $\Delta = 4$ .

Lemma 8 (used with  $k = 2$  and  $\Delta = 3$ ) implies that there does not exist (assuming  $\text{NP} \neq \text{RP}$ ) an FPRAS for the partition function of the hard-core model with activity  $\lambda > \sqrt{5} - 1$  in graphs of maximum degree 6.

The range of  $\lambda$  for  $\Delta$  and  $\Delta - 1$  where we can prove hardness (that is,  $(\lambda_c(\mathbb{T}_\Delta), \lambda_c(\mathbb{T}_{\Delta-1}))$ ) overlap for  $\Delta \geq 6$ . This is useful since the hardness for  $\Delta - 1$  automatically gives hardness for  $\Delta$ .

Thus for  $\Delta \geq 6$  we have the hardness result on the set

$$(\lambda_c(\mathbb{T}_\Delta), \lambda_c(\mathbb{T}_{\Delta-1})] \cup \dots \cup (\lambda_c(\mathbb{T}_6), \lambda_c(\mathbb{T}_5)] \cup (\lambda_c(\mathbb{T}_5), \lambda_c(\mathbb{T}_5) + 0.402912] \cup (\sqrt{5} - 1, \infty) = (\lambda_c(\mathbb{T}_\Delta), \infty).$$

This concludes the proof of the theorem for  $\Delta \geq 6$ .

For  $\Delta = 4$ , we have the hardness result on the set  $(\lambda_c(\mathbb{T}_4), 2.01538] \cup (4, +\infty)$ .

For  $\Delta = 5$ , we have the hardness result on the set

$$(\lambda_c(\mathbb{T}_5), 1.45641] \cup (1.6875, 2.01538] \cup (4, +\infty).$$

$\square$

## 2.5 On the Use of Computational Assistance

We use Mathematica to prove several inequalities involving rational functions in regions bounded by rational functions. Such inequalities are known to be decidable by Tarski's quantifier elimination [14], the particular version of Collins algebraic decomposition (CAD) used by Mathematica's `Resolve` command is described in [13]. The algorithms are guaranteed to return correct answers—they do not suffer from precision issues since they use interval arithmetic (a real number is represented using an interval whose endpoints are rational numbers).

### 3 Non-Reconstruction revisited

In this section, we reprove Lemma 4.2 from Sly [11] without (9) in the hypothesis. This will allow us to focus on proving Lemma 5.

Recall,  $\mathbb{T}_\Delta$  is the infinite  $\Delta$ -regular tree, and  $p^+, p^-$  denote the marginal probabilities that the root is occupied for the limit of even and odd, respectively, sized trees. Let  $\hat{\mathbb{T}}_\Delta$  denote the infinite  $(\Delta - 1)$ -ary tree rooted at  $\rho$ . (Thus, these two trees only differ at the root.) For  $\ell \in \mathbb{N}$ , let  $\hat{T}_\ell$  denote the tree with branching factor  $\Delta - 1$  and containing  $\ell$  levels. Let  $q_\ell$  denote the marginal probability that the root is occupied in the Gibbs distribution on  $\hat{T}_\ell$ . Analogous to  $p^+$  and  $p^-$ , let

$$q^+ = \lim_{\ell \rightarrow \infty} q_{2\ell} \quad \text{and} \quad q^- = \lim_{\ell \rightarrow \infty} q_{2\ell+1}.$$

The densities  $q^+, q^-$  are related to  $p^+, p^-$  by:

$$q^+ = \frac{p^+}{1 - p^-}, \quad q^- = \frac{p^-}{1 - p^+}.$$

There are two semi-translation invariant measures  $\hat{\mu}^+$  and  $\hat{\mu}^-$  on  $\hat{\mathbb{T}}_\Delta$  obtained by taking the weak limit of the hard-core measure of even-sized trees  $\hat{T}_{2\ell}$  and odd-sized trees  $\hat{T}_{2\ell+1}$ , respectively. In these measures  $\hat{\mu}^+, \hat{\mu}^-$  on the infinite tree,  $q^+$  and  $q^-$ , respectively, are the marginal probabilities that the root is occupied. These measures  $\hat{\mu}^+$  and  $\hat{\mu}^-$  can also be generated by a broadcasting process, see [11, Section 4].

For  $v \in \hat{\mathbb{T}}_\Delta$ , denote by  $S_{v,\ell}$  the vertices at level  $\ell$  in the subtree of  $\hat{\mathbb{T}}_\Delta$  rooted at  $v$ . Let  $X_{\rho,\ell,+}$  denote the marginal probability that the root  $\rho$  is occupied in an independent set  $X$  generated by the following process: we first sample an independent set  $\hat{X}$  from the measure  $\hat{\mu}^+$ , then we condition on the configuration  $\hat{X}_S$  on  $S_{\rho,\ell}$ , and finally we sample an independent set  $X$  from the hard-core measure on  $\hat{T}_\ell$  conditioned on  $X_S = \hat{X}_S$ . Note that the configuration of the vertices in  $S_{\rho,\ell}$  is a random vector, so that  $X_{\rho,\ell,+}$  is a random variable. Define similarly  $X_{\rho,\ell,-}$  for  $\hat{\mu}^-$ .

We may extend this definition to an arbitrary vertex  $v \in \hat{\mathbb{T}}_\Delta$  at distance  $D$  from the root  $\rho$ , by setting  $X_{v,\ell,+} = X_{\rho,\ell,+}$  if  $D$  is even or  $X_{v,\ell,+} = X_{\rho,\ell,-}$  if  $D$  is odd. Thus,  $X_{v,\ell,+}$  is the probability that, in an appropriate translation of  $\hat{\mu}^+$ ,  $v$  is occupied conditioning on the configuration of  $S_{v,\ell}$ . Define similarly  $X_{v,\ell,-}$  for  $\hat{\mu}^-$ .

In Sly [11], it is proved that  $X_{\rho,\ell,+}$  ( $X_{\rho,\ell,-}$ ) is strongly concentrated around  $q^+$  ( $q^-$ , respectively) under the condition that  $p^+ < \frac{3}{5}(1 - p^-)$ . This concentration is used by Sly for establishing the properties of the gadget he uses in his reduction. We need to reprove the concentration without the condition  $p^+ < \frac{3}{5}(1 - p^-)$ .

**Lemma 9** (see Lemma 4.2 in Sly [11]). *When  $\lambda > \lambda_c(\mathbb{T}_\Delta)$ , there exist constants  $\zeta_1(\lambda, \Delta), \zeta_2(\lambda, \Delta) > 0$ , for all sufficiently large  $\ell$ ,*

$$\begin{aligned} \mathbb{P} \left[ \left| X_{\rho,\ell,+} - q^+ \right| \geq \exp(-\zeta_1 \ell) \right] &\leq \exp(-\exp(\zeta_2 \ell)). \\ \mathbb{P} \left[ \left| X_{\rho,\ell,-} - q^- \right| \geq \exp(-\zeta_1 \ell) \right] &\leq \exp(-\exp(\zeta_2 \ell)). \end{aligned}$$

*Proof.* We follow the proof of [11]. For a vertex  $v \in \hat{\mathbb{T}}_\Delta$ , let  $N(v) = N^1(v)$  denote its children, and for  $i \in \mathbb{N}$ , let  $N^i(v)$  denote its descendants  $i$  levels below. For  $1 \leq i \leq \ell$  and  $s \in \{+, -\}$ , let  $\mathcal{X}_{N^i(v), \ell-i, s}$  denote the vector  $\{X_{w, \ell-i, s} : w \in N^i(v)\}$ .

By standard tree recursions, it can be proved that for  $s \in \{+, -\}$ ,

$$X_{v,\ell,s} = h(\mathcal{X}_{N(v), \ell-1, s}) := \frac{\lambda \prod_{w \in N(v)} (1 - X_{w, \ell-1, s})}{1 + \lambda \prod_{w \in N(v)} (1 - X_{w, \ell-1, s})}.$$

In our framework, one may establish a contraction property for  $h$ , but it is slightly more straightforward to look at depth two of the recursion. Note that

$$1 - X_{v,\ell,s} = \frac{1}{1 + \lambda \prod_{w \in N(v)} (1 - X_{w,\ell-1,s})}$$

so that

$$\begin{aligned} X_{v,\ell,s} &= 1 - \frac{1}{1 + \lambda \prod_{w \in N(v)} \frac{1}{1 + \lambda \prod_{z \in N(w)} (1 - X_{z,\ell-2,s})}} \\ &= \frac{\lambda}{\lambda + \prod_{w \in N(v)} \left( 1 + \lambda \prod_{z \in N(w)} (1 - X_{z,\ell-2,s}) \right)} \\ &=: r(\mathcal{X}_{N^2(\rho),\ell-2,s}). \end{aligned} \tag{10}$$

By recursively applying (10), we obtain that

$$X_{\rho,\ell,s} =: g(\mathcal{X}_{N^{2L}(\rho),\ell-2L,s}).$$

Note that  $r(\mathcal{X}_{N^2(\rho),\ell-2,s}) = g(\mathcal{X}_{N^2(\rho),\ell-2,s})$ .

For the rest of the proof, we focus on the case  $s = +$  and  $v$  being at even distance from the root  $\rho$ , the other cases being almost identical (since we are looking at depth two of the recursion).

Assume  $\mathcal{X}_{N^2(v),\ell-2,+}$ ,  $\mathcal{X}'_{N^2(v),\ell-2,+}$  are two vectors which are equal except at one vertex  $z^* \in N^2(v)$ . To prove the new version of the lemma, it suffices to obtain the following contraction property. We will prove for all  $\ell$  sufficiently large, for all  $v \in \hat{\mathbb{T}}_\Delta$ , for all pairs  $\mathcal{X}_{N^2(v),\ell-2,+}$ ,  $\mathcal{X}'_{N^2(v),\ell-2,+}$  that differ at a single vertex  $z^*$ ,

$$|r(\mathcal{X}_{N^2(v),\ell-2,+}) - r(\mathcal{X}'_{N^2(v),\ell-2,+})| \leq \left( \frac{1}{(\Delta-1)^2} + \frac{1}{10} \right) |X_{z^*,\ell-2,+} - X'_{z^*,\ell-2,+}|. \tag{11}$$

To accomplish this, it suffices to prove that for  $\ell$  large enough, it holds that:

$$\left| \frac{\partial r}{\partial X_{z^*,\ell-2,+}}(\mathcal{X}_{N^2(v),\ell-2,+}) \right| < \frac{1}{(\Delta-1)^2} + \frac{1}{10}. \tag{12}$$

Let  $w^* \in N(v)$  be the parent of  $z^*$ . Then (12) is equivalent to:

$$\frac{\lambda^2 \prod_{z \in N(w^*) \setminus \{z^*\}} (1 - X_{z,\ell-2,+}) \prod_{w \in N(v) \setminus \{w^*\}} \left( 1 + \lambda \prod_{z \in N(w)} (1 - X_{z,\ell-2,+}) \right)}{\left[ \lambda + \prod_{w \in N(v)} \left( 1 + \lambda \prod_{z \in N(w)} (1 - X_{z,\ell-2,+}) \right) \right]^2} < \frac{1}{(\Delta-1)^2} + \frac{1}{10}.$$

Note that as  $\ell \rightarrow +\infty$ , since  $v$  is at even distance from  $\rho$ ,  $X_{v,\ell,+}$  converges almost surely to  $q^+$  (see [11, equation (4.1)] and [11, proof of Lemma 4.2]). Hence, as  $\ell \rightarrow +\infty$ , we have that

$$\left| \frac{\partial r}{\partial X_{z^*,\ell-2,+}}(\mathcal{X}_{N^2,\ell-2,+}) \right| \rightarrow \frac{\lambda^2 (1 - q^+)^{\Delta-2} (1 + \lambda (1 - q^+)^{\Delta-1})^{\Delta-2}}{\left[ \lambda + (1 + \lambda (1 - q^+)^{\Delta-1})^{\Delta-1} \right]^2} =: \gamma.$$

Pick  $\ell_0 = \ell_0(\Delta, \lambda)$  so that for all  $\ell \geq \ell_0$  we have that

$$\left| \frac{\partial r}{\partial X_{z^*,\ell-2,+}}(\mathcal{X}_{N^2(v),\ell-2,+}) - \gamma \right| \leq \frac{1}{10}.$$

We will see next that  $\gamma = q^+q^-$  and hence by Part 3 of Lemma 4, it follows that  $\gamma \leq \frac{1}{(\Delta-1)^2}$  which proves (12).

To see that  $\gamma = q^+q^-$ , note that  $\lambda(1-q^+)^{\Delta-1} = \frac{q^-}{1-q^-}$  and  $\lambda(1-q^-)^{\Delta-1} = \frac{q^+}{1-q^+}$  (one can derive these equalities by  $p^+ = \phi(p^-)$ ,  $p^- = \phi(p^+)$ , see Part 1 of Lemma 4). It is now a matter of a few algebra substitutions to check that  $\gamma = q^+q^-$ .

This proves (11). Recursively applying this relation (11) implies that for all  $\ell - L > \ell_0$ , for  $\Delta \geq 3$ ,

$$|g(\mathcal{X}_{N^L(v), \ell-L, +}) - g(\mathcal{X}'_{N^L(v), \ell-L, +})| \leq \left(\frac{1}{2}\right)^{\lfloor L/2 \rfloor} |X_{z^*, \ell-L, +} - X'_{z^*, \ell-L, +}|. \quad (13)$$

Having established (13), the rest of Sly's proof of Lemma 4.2 goes through.  $\square$

## 4 Analysis of the Second Moment

In this section, we prove Lemma 5. We break its proof into two slightly easier components, namely Lemmata 10 and 11 stated below, depending on the value of  $p^+$ . Notice that Lemma 10 determines explicitly a region of  $(\alpha, \beta)$  for which Condition 1 holds.

**Lemma 10.** *Let  $\Delta \geq 3$  and let  $(\alpha, \beta) \in \mathcal{R}_\Delta$ ,  $\alpha, \beta > 0$ , and  $\alpha, \beta \leq 1/2$ . Then  $g_{\alpha, \beta}(\gamma, \delta, \varepsilon) := \Phi_2(\alpha, \beta, \gamma, \delta, \varepsilon)$  achieves its unique maximum in the region (3) at the point  $(\gamma^*, \delta^*, \varepsilon^*)$ .*

**Lemma 11.** *Fix  $\Delta = 3$  and  $\lambda > \lambda_c(\mathbb{T}_\Delta)$ . Let  $p^+$  and  $p^-$  be the corresponding probabilities. Assume that  $1/2 \leq p^+ < 1$ . There exists a constant  $\chi > 0$  such that for  $|p^+ - \alpha| < \chi$  and  $|p^- - \beta| < \chi$ ,  $g_{\alpha, \beta}(\gamma, \delta, \varepsilon) := \Phi_2(\alpha, \beta, \gamma, \delta, \varepsilon)$  achieves its unique maximum in the region (3) at the point  $(\gamma^*, \delta^*, \varepsilon^*)$ .*

*Proof of Lemma 5.* We begin by proving the second part of the lemma ( $\Delta > 3$  case) and then we prove the first part ( $\Delta = 3$  case).

Fix any  $\Delta \geq 3$  and  $\lambda > \lambda_c(\mathbb{T}_\Delta)$ . Let  $p^+$ ,  $p^-$  be the corresponding marginal probabilities that the root is occupied in the measures  $\mu^+$ ,  $\mu^-$ . By the third item of Lemma 4, we have that  $(\alpha, \beta) = (p^+, p^-)$  is contained in the interior of  $\mathcal{R}_\Delta$ . Hence, the same holds for every  $(\alpha, \beta)$  in a small enough neighborhood of  $(p^+, p^-)$ . Hence, provided that  $p^+ \leq 1/2$ , Lemma 10 verifies the condition for any such point. It is now easy to see that  $p^+$  is increasing in  $\lambda$ , and hence  $p^+ \leq 1/2$  iff  $\lambda \in (\lambda_c(\mathbb{T}_\Delta), \lambda_{1/2}(\mathbb{T}_\Delta)]$ . This proves the second part of Lemma 5.

The first part of Lemma 5 is proved analogously. When  $p^+ \leq 1/2$ , one uses Lemma 10 as above, while when  $p^+ \geq 1/2$  the condition reduces to Lemma 11.  $\square$

Thus we may focus our attention on proving Lemmata 10 and 11. While the analysis at some point for Lemma 11 requires tighter arguments, the two proofs share many common preprocessing steps. The rest of this section is devoted to these common preprocessing steps and the proofs of Lemmata 10 and 11 are given in Section 5.

#### 4.1 The Partial Derivatives

The derivatives of  $\Phi_2$  with respect to  $\gamma, \delta, \varepsilon$  can easily be computed and are also given in [10, Proof of Lemma 6.1]:

$$\exp\left(\frac{\partial\Phi_2}{\partial\gamma}\right) = \frac{(1-2\beta+\delta-\gamma-\varepsilon)^\Delta(\alpha-\gamma-\varepsilon)^\Delta(1-2\alpha+\gamma)^{\Delta-1}}{(1-\beta-\gamma-\varepsilon)^\Delta(\beta-\alpha+\gamma-\delta+\varepsilon)^\Delta(\alpha-\gamma)^{\Delta-2}\gamma}, \quad (14)$$

$$\exp\left(\frac{\partial\Phi_2}{\partial\delta}\right) = \frac{(\beta-\alpha-\delta+\gamma+\varepsilon)^\Delta(1-2\beta+\delta)^{\Delta-1}}{(1-2\beta+\delta-\gamma-\varepsilon)^\Delta(\beta-\delta)^{\Delta-2}\delta}, \quad (15)$$

$$\exp\left(\frac{\partial\Phi_2}{\partial\varepsilon}\right) = \frac{(1-2\beta+\delta-\gamma-\varepsilon)^\Delta(\alpha-\gamma-\varepsilon)^\Delta(1-\alpha-\beta-\varepsilon)^\Delta}{\varepsilon^\Delta(\beta-\alpha-\delta+\gamma+\varepsilon)^\Delta(1-\beta-\gamma-\varepsilon)^\Delta}. \quad (16)$$

#### 4.2 Excluding the Boundary of the Region

We argue that for  $(\alpha, \beta) \in \mathcal{R}_\Delta$ , the maximum of  $g_{\alpha, \beta}$  cannot occur on the boundary of the region defined by (3).

**Lemma 12.** *For every  $\Delta \geq 3$  and  $(\alpha, \beta) \in \mathcal{R}_\Delta$ ,  $g_{\alpha, \beta}(\gamma, \delta, \varepsilon) := \Phi_2(\alpha, \beta, \gamma, \delta, \varepsilon)$  attains its maximum in the interior of (3).*

*Proof.* We follow the proof of Lemma 6.1 of [10] (where the same result is proved in the special case  $\alpha = \beta = \frac{1}{\Delta}$ ).

We will prove that  $g_{\alpha, \beta}(\gamma, \delta, \varepsilon)$  attains its maximum in the interior of (3) by showing that at least one derivative in (14)–(16) goes to infinity (+ or – according to the direction), as we approach one of the boundaries defined by (3) from the interior of (3).

For  $\Delta \geq 3$ , note that  $(\alpha, \beta) \in \mathcal{R}_\Delta$  implies  $\alpha + \beta < 1$ . Without loss of generality, we assume that  $\alpha \geq \beta$ . Hence  $\beta < 1/2$ . We have (15) goes to  $+\infty$  as  $\delta \rightarrow 0$ , and (16) goes to  $+\infty$  as  $\varepsilon \rightarrow 0$ . We also have (16) goes to  $-\infty$  as  $\gamma + \varepsilon \rightarrow \alpha$ , (15) goes to  $-\infty$  as  $\delta \rightarrow \beta$ , (16) goes to  $-\infty$  as  $\gamma + \varepsilon - \delta \rightarrow 1 - 2\beta$ , (16) goes to  $-\infty$  as  $\varepsilon \rightarrow 1 - \alpha - \beta$ , and (16) goes to  $+\infty$  as  $\gamma + \varepsilon - \delta \rightarrow \alpha - \beta$ .

When  $\alpha \geq 1/2$ , the condition  $\gamma = 0$  is not a boundary, as  $\gamma \geq 0$  is implied by the conditions  $\delta \geq 0$ ,  $1 - \alpha - \beta - \varepsilon \geq 0$ , and  $\beta - \delta + \varepsilon + \gamma - \alpha \geq 0$ . On the other hand, when  $\alpha < 1/2$ , we have (14) goes to  $+\infty$  as  $\gamma \rightarrow 0$ .  $\square$

#### 4.3 Eliminating one variable

Fix  $\Delta, \alpha, \beta, \gamma, \delta$  and view  $\Phi_2$  as a function of  $\varepsilon$ . We maximize with respect to  $\varepsilon$ . In this setting, it was proved [10, Lemma 6.3], that the only maximizer of the function  $\Phi_2$  in the interior of (3) is obtained by solving  $\frac{\partial\Phi_2}{\partial\varepsilon} = 0$  and is given by:

$$\hat{\varepsilon} := \hat{\varepsilon}(\alpha, \beta, \gamma, \delta) = \frac{1}{2}(1 + \alpha - \beta - 2\gamma - \sqrt{D}), \quad (17)$$

where

$$\begin{aligned} D &= (1 + \alpha - \beta - 2\gamma)^2 - 4(\alpha - \gamma)(1 - 2\beta - \gamma + \delta) \\ &= (\alpha + \beta - 1)^2 + 4(\alpha - \gamma)(\beta - \delta). \end{aligned}$$

Define

$$\hat{\eta} := \hat{\eta}(\alpha, \beta, \gamma, \delta) = \frac{1}{2}(1 - \alpha + \beta - 2\delta - \sqrt{D}), \quad (18)$$

and note that

$$\begin{aligned}\alpha - \gamma - \hat{\varepsilon} &= \beta - \delta - \hat{\eta} = \frac{1}{2}(-(1 - \alpha - \beta) + \sqrt{D}), \\ (\alpha - \gamma - \hat{\varepsilon})(1 - \alpha - \beta - \hat{\varepsilon} - \hat{\eta}) &= \hat{\varepsilon}\hat{\eta}.\end{aligned}\tag{19}$$

The new parameter  $\hat{\eta}$  (not used in [10]) is symmetric with  $\hat{\varepsilon}$ , i.e, the constraints and formulas we have are invariant under a symmetry that swaps  $\alpha, \gamma, \hat{\varepsilon}$  with  $\beta, \delta, \hat{\eta}$ . This will allow for simpler arguments (using the symmetry).

From the previous discussion and equation (17), we may eliminate variable  $\varepsilon$  of our consideration. Of course, this introduces some complexity due to the radical  $\sqrt{D}$ , but still this is manageable. Let

$$f(\gamma, \delta) := g_{\alpha, \beta}(\gamma, \delta, \hat{\varepsilon}) = \Phi_2(\alpha, \beta, \gamma, \delta, \hat{\varepsilon}).$$

To prove that  $(\gamma^*, \delta^*, \varepsilon^*)$  is the unique global maximum of  $g_{\alpha, \beta}$  in the interior of the region defined by (3), it suffices to prove that  $(\gamma^*, \delta^*)$  is the unique global maximum of  $f$  for  $(\gamma, \delta)$  in the interior of the following region, which contains the  $(\gamma, \delta)$ -projection of the region defined by (3):

$$0 \leq \gamma \leq \alpha, \quad 0 \leq \delta \leq \beta, \quad 0 \leq 1 - 2\beta + \delta - \gamma, \quad 0 \leq 1 - 2\alpha + \gamma - \delta.\tag{20}$$

Each inequality in (20) is implied by the inequalities in (3), the only non-trivial case being the last inequality which is the sum of  $1 - \alpha - \beta - \varepsilon \geq 0$  and  $\beta - \delta + \varepsilon + \gamma - \alpha \geq 0$ .

The first derivatives of  $f$  with respect to  $\gamma, \delta$  are

$$\frac{\partial f}{\partial \gamma}(\gamma, \delta) = \Delta \ln W_{11} + \ln W_{12},\tag{21}$$

$$\frac{\partial f}{\partial \delta}(\gamma, \delta) = \Delta \ln W_{21} + \ln W_{22},\tag{22}$$

where

$$\begin{aligned}W_{11} &= \frac{(\alpha - \gamma - \hat{\varepsilon})\hat{\varepsilon}(1 - 2\alpha + \gamma)}{\hat{\eta}(\alpha - \gamma)^2} = \frac{\hat{\varepsilon}(1 - 2\alpha + \gamma)}{(1 - \alpha - \beta - \hat{\varepsilon})(\alpha - \gamma)}, & W_{12} &= \frac{(\alpha - \gamma)^2}{(1 - 2\alpha + \gamma)\gamma}, \\ W_{21} &= \frac{(\beta - \delta - \hat{\eta})\hat{\eta}(1 - 2\beta + \delta)}{\hat{\varepsilon}(\beta - \delta)^2} = \frac{\hat{\eta}(1 - 2\beta + \delta)}{(1 - \alpha - \beta - \hat{\eta})(\beta - \delta)}, & W_{22} &= \frac{(\beta - \delta)^2}{(1 - 2\beta + \delta)\delta}.\end{aligned}$$

Note that the rightmost equalities in the definition of  $W_{11}$  and  $W_{21}$  follow from (18) and (19).

For every  $\Delta \geq 3$ , and  $(\alpha, \beta) \in \mathcal{R}_\Delta$ , we have that  $(\gamma^*, \delta^*)$  is a stationary point of  $f$  (this follows from the fact that for  $\gamma = \alpha^2$  and  $\delta = \beta^2$ , the inequalities on the right-hand sides in Lemma 13 become equalities, and from (21), (22) we have that the derivatives of  $f$  vanish).

#### 4.4 Restricting the Region

To determine whether (21) and (22) are zero it will be useful to understand conditions that make  $W_{11}, W_{12}, W_{21}, W_{22}$  greater or equal to 1. The following lemma gives such conditions. The proof is given in Section 6.1.

**Lemma 13.** *For every  $(\alpha, \beta) \in \mathcal{R}$ , and  $(\gamma, \delta)$  in the interior of (20),*

$$\begin{aligned}W_{11} \geq 1 &\iff (1 - \alpha)^2\delta + \beta^2(2\alpha - 1 - \gamma) \geq 0, \\ W_{12} \geq 1 &\iff \gamma \leq \alpha^2, \\ W_{21} \geq 1 &\iff (1 - \beta)^2\gamma + \alpha^2(2\beta - 1 - \delta) \geq 0, \\ W_{22} \geq 1 &\iff \delta \leq \beta^2.\end{aligned}$$

By considering the sign of (21) and (22) and Lemma 13, we have that the stationary points of  $f$  (and hence of  $g_{\alpha,\beta}$ ) can only be in

$$0 < \gamma \leq \alpha^2, \quad 0 < \delta \leq \beta^2, \quad (1 - \alpha)^2 \delta + \beta^2(2\alpha - 1 - \gamma) \leq 0, \quad (1 - \beta)^2 \gamma + \alpha^2(2\beta - 1 - \delta) \leq 0, \quad (23)$$

or

$$\alpha^2 \leq \gamma < \alpha, \quad \beta^2 \leq \delta < \beta, \quad (1 - \alpha)^2 \delta + \beta^2(2\alpha - 1 - \gamma) \geq 0, \quad (1 - \beta)^2 \gamma + \alpha^2(2\beta - 1 - \delta) \geq 0. \quad (24)$$

Note that for  $\gamma = \alpha^2, \delta = \beta^2$  one has  $W_{11} = W_{12} = W_{21} = W_{22} = 1$  (Lemma 13 holds with equalities as well instead of inequalities), so that  $(\alpha^2, \beta^2)$  is always a stationary point for  $f(\gamma, \delta)$ .

#### 4.5 The Hessian

To prove that  $f$  has a unique maximum, we are going to argue that  $f$  is strictly concave in each of the regions defined by (23) and (24). It will thus be crucial to study the Hessian of  $f$ .

Let  $\mathbf{H}$  denote the Hessian of  $f$ , i.e.,

$$\mathbf{H} = \begin{pmatrix} \frac{\partial^2 f}{\partial \gamma^2}(\gamma, \delta) & \frac{\partial^2 f}{\partial \gamma \partial \delta}(\gamma, \delta) \\ \frac{\partial^2 f}{\partial \delta \partial \gamma}(\gamma, \delta) & \frac{\partial^2 f}{\partial \delta^2}(\gamma, \delta) \end{pmatrix}.$$

Our goal is to express  $\mathbf{H}$  in a helpful explicit form. In this vein, it will be convenient to define the following quantities.

$$\begin{aligned} R_1 &= \frac{1-\alpha-\beta}{1-\alpha-\beta-\varepsilon-\eta}, & R_2 &= \frac{\sqrt{D}}{1-2\alpha+\gamma}, & R_3 &= \frac{2(\alpha-\gamma-\varepsilon)}{\alpha-\gamma}, \\ R_4 &= \frac{\sqrt{D}}{\gamma}, & R_5 &= \frac{2(1-\beta-\gamma-\varepsilon)}{\alpha-\gamma}, & R_6 &= \frac{\sqrt{D}}{1-2\beta+\delta}, \\ R_7 &= \frac{2(\alpha-\gamma-\varepsilon)}{\beta-\delta}, & R_8 &= \frac{\sqrt{D}}{\delta}, & R_9 &= \frac{2(1-\beta-\gamma-\varepsilon)}{\beta-\delta}. \end{aligned}$$

$\mathbf{H}$  can now be written in a relatively nice form with respect to the  $R_i$ . Namely,

$$\frac{\partial^2 f}{\partial \gamma^2}(\gamma, \delta) = \frac{1}{\sqrt{D}} \left[ (-R_1 + R_2 + R_3)\Delta - R_2 - R_3 - R_4 - R_5 \right], \quad (25)$$

$$\frac{\partial^2 f}{\partial \delta^2}(\gamma, \delta) = \frac{1}{\sqrt{D}} \left[ (-R_1 + R_6 + R_7)\Delta - R_6 - R_7 - R_8 - R_9 \right], \quad (26)$$

$$\frac{\partial^2 f}{\partial \gamma \partial \delta}(\gamma, \delta) = \frac{\partial f}{\partial \delta \partial \gamma}(\gamma, \delta) = \frac{\Delta R_1}{\sqrt{D}}. \quad (27)$$

Inspecting the  $R_i$  we obtain the following observation.

**Observation 14.**  $R_1, \dots, R_9$  are positive when  $(\alpha, \beta) \in \mathcal{R}_\Delta$  and  $(\gamma, \delta)$  in the interior of (20).

Observation 14 and equation (27) immediately yield:

**Observation 15.** For every  $(\alpha, \beta) \in \mathcal{R}_\Delta$ , and  $(\gamma, \delta)$  in the interior of (20),

$$\frac{\partial^2 f}{\partial \gamma \partial \delta}(\gamma, \delta) = \frac{\partial f}{\partial \delta \partial \gamma}(\gamma, \delta) > 0.$$

In Section 6.2 we prove the following technical inequality on the  $R_i$ .

**Lemma 16.** For every  $(\alpha, \beta) \in \mathcal{R}$ , and  $(\gamma, \delta)$  in the interior of (20),

$$R_1 > R_2 + R_3, \quad \text{and} \quad R_1 > R_6 + R_7.$$



Applying Lemma 16 and Observation 14, (25) and (26) give the following straightforward corollary.

**Corollary 17.** *For every  $(\alpha, \beta) \in \mathcal{R}$ , and  $(\gamma, \delta)$  in the interior of (20),*

$$\frac{\partial f}{\partial^2 \gamma}(\gamma, \delta) < 0, \quad \frac{\partial f}{\partial^2 \delta}(\gamma, \delta) < 0.$$

Corollary 17 implies that the sum of the eigenvalues of  $\mathbf{H}$  is negative. Hence,  $\mathbf{H}$  is negative definite iff the determinant of  $\mathbf{H}$  is negative. We have the following expression for  $\det(\mathbf{H})$ .

$$\begin{aligned} \det(\mathbf{H}) &= \frac{\partial f}{\partial^2 \gamma}(\gamma, \delta) \cdot \frac{\partial f}{\partial^2 \delta}(\gamma, \delta) - \frac{\partial f}{\partial \gamma \partial \delta}(\gamma, \delta) \cdot \frac{\partial f}{\partial \delta \partial \gamma}(\gamma, \delta) \\ &= \frac{1}{D} \left\{ (\Delta - 1)^2 \left[ (-R_1 + R_2 + R_3)(-R_1 + R_6 + R_7) - R_1^2 \right] \right. \\ &\quad \left. + (\Delta - 1) \left[ (-R_1 + R_2 + R_3)(-R_1 - R_8 - R_9) + \right. \right. \\ &\quad \left. \left. + (-R_1 + R_6 + R_7)(-R_1 - R_4 - R_5) - 2R_1^2 \right] \right. \\ &\quad \left. + \left[ (-R_1 - R_8 - R_9)(-R_1 - R_4 - R_5) - R_1^2 \right] \right\}. \end{aligned} \quad (28)$$

## 5 Concluding the Proofs of Lemmata 10 and 11

In this section, we give the proofs of Lemmata 10 and 11. We first recap what we have accomplished in Section 4 for every  $(\alpha, \beta) \in \mathcal{R}_\Delta$ .

1. The function  $g_{\alpha, \beta}(\gamma, \delta, \varepsilon)$  attains its maximum in the interior of the region (3). See Section 4.2.
2. To study the (local) maxima of  $g$  in the interior of the region (3), it suffices to study the maxima of the function  $f(\gamma, \delta) = g_{\alpha, \beta}(\gamma, \delta, \varepsilon)$  in the interior of the region (20). More explicitly, if  $f(\gamma, \delta)$  has a unique maximum in the interior of the region (20) at  $(\gamma^*, \delta^*) = (\alpha^2, \beta^2)$ , then  $g_{\alpha, \beta}$  has a unique maximum in the interior of the region (3) at  $(\gamma^*, \delta^*, \varepsilon^*) = (\alpha^2, \beta^2, \alpha(1 - \alpha - \beta))$ . The function  $f$  is differentiable in the interior of the region (20). See Section 4.3.
3. The point  $(\gamma^*, \delta^*) = (\alpha^2, \beta^2)$  is always stationary for  $f$ . Every stationary point of  $f$  lies in one of the two regions defined by (i) (20) and (23), (ii) (20) and (24). See Section 4.4.
4. The function  $f$  is strictly concave iff  $\det(\mathbf{H}) > 0$ . See Section 4.5.

By the above discussion, if for some  $(\alpha, \beta) \in \mathcal{R}_\Delta$  it holds that  $f$  is strictly concave in each of the regions (i) (20) and (23), (ii) (20) and (24), then  $g_{\alpha, \beta}$  has a unique maximum at  $(\gamma^*, \delta^*, \varepsilon^*) = (\alpha^2, \beta^2, \alpha(1 - \alpha - \beta))$ . Thus, it suffices to check that  $\det(\mathbf{H}) > 0$  in each of these regions. This is essentially the way we derive Lemmata 10 and 11.

Hence, the main challenge is proving that  $\det(\mathbf{H}) > 0$ . This can be done slightly more easily in the region (20) and (23). Indeed, in Section 6.3 we prove the following lemma.

**Lemma 18.**  *$\det(\mathbf{H}) > 0$  for every  $\Delta \geq 3$ ,  $(\alpha, \beta) \in \mathcal{R}_\Delta$ ,  $(\gamma, \delta)$  in the interior of (20) and  $(\gamma, \delta)$  in (23).*

Proving  $\det(\mathbf{H}) > 0$  in the intersection of the regions (20) and (23) is trickier and is essentially the reason we do not obtain our hardness result for  $\Delta = 4, 5$ . At this point, it is convenient to split the analysis for each of the lemmas.

## 5.1 Proof of Lemma 10

In the setup of Lemma 10, we have  $(\alpha, \beta) \in \mathcal{R}_\Delta$  and  $\alpha, \beta \leq 1/2$ . We suppress the details of proving  $\det(\mathbf{H}) > 0$  as a lemma, whose proof we defer to Section 6.4.

**Lemma 19.**  $\det(\mathbf{H}) > 0$  for every  $\Delta \geq 3$ ,  $(\alpha, \beta) \in \mathcal{R}_\Delta$ ,  $\alpha, \beta \leq 1/2$ ,  $(\gamma, \delta)$  in the interior of (20) and  $(\gamma, \delta)$  in (24).

Using Lemmata 18 and 19, the proof of Lemma 10 is immediate.

*Proof of Lemma 10.* Lemma 18 and Lemma 19 imply that  $f$  has a unique maximum at  $(\gamma^*, \delta^*)$  for every  $\Delta \geq 3$ ,  $(\alpha, \beta) \in \mathcal{R}_\Delta$ ,  $1/2 \geq \alpha, \beta$  and  $(\gamma, \delta)$  in the interior of (20). This follows from the fact that  $\det(\mathbf{H}) > 0$  implies that the Hessian of  $f$  is negative definite in the region of interest, i.e., where  $g_{\alpha, \beta}$  could possibly have stationary points, which in turn implies that  $f$  is strictly concave in the region and hence has a unique maximum. By the definition of  $f$ , it follows that  $g_{\alpha, \beta}$  has a unique maximum at  $(\gamma^*, \delta^*, \varepsilon^*)$ . For a more thorough outline, see the beginning of Section 5.  $\square$

## 5.2 Proof of Lemma 11

In the setup of Lemma 11, we have  $\Delta = 3$  and  $p^+ \geq 1/2$ . By (1), tedious but otherwise simple algebra gives that the solution of  $\beta = \phi(\alpha)$  and  $\alpha = \phi(\beta)$  with  $\alpha \neq \beta$  satisfies

$$\alpha^2 - 2\alpha + \alpha\beta + 1 - 2\beta + \beta^2 = 0.$$

It can also be checked that when  $1 > p^+ \geq 1/2$ , it holds that  $0 < p^- \leq (3 - \sqrt{5})/4$ . Define  $\mathcal{R}'_3$  to be the set of pairs  $(\alpha, \beta)$  such that  $\alpha^2 - 2\alpha + \alpha\beta + 1 - 2\beta + \beta^2 = 0$ ,  $1/2 \leq \alpha < 1$  and  $0 < \beta \leq (3 - \sqrt{5})/4$ . Our goal is to show that  $\det(\mathbf{H}) > 0$  for every  $(\alpha, \beta) \in \mathcal{R}'_3$ ,  $(\gamma, \delta)$  in the interior of (20) and  $(\gamma, \delta)$  in (24).

We can rewrite  $\det(\mathbf{H})$  using the formula in (28) as

$$\begin{aligned} \det(\mathbf{H}) &= \frac{1}{D} \left[ 3R_1(U_1 + U_2) + U_1U_2 \right] \\ &= \frac{U_1}{D} \left[ 3R_1(1 + U_2/U_1) + U_2 \right], \end{aligned} \tag{29}$$

where

$$U_1 = R_8 + R_9 - 2R_6 - 2R_7, \quad U_2 = R_4 + R_5 - 2R_2 - 2R_3.$$

The following lemma establishes technical inequalities on  $U_1, U_2, R_1, \dots, R_9$ , which are crucial in establishing the positivity of  $\det(\mathbf{H})$ . Its proof is given in Section 6.5.

**Lemma 20.** We have  $U_1 > 0$ ,  $R_4 > R_6$ ,  $R_5 > R_7$ ,  $R_5 > 4R_3$ ,  $R_9 > 4R_7$ , and  $3R_8/2 + R_9 > 9R_2$ , for every  $(\alpha, \beta) \in \mathcal{R}'_3$ ,  $(\gamma, \delta)$  in the interior of (20) and  $(\gamma, \delta)$  in (24).

With Lemma 20 at hand, we can now prove that  $\det(\mathbf{H})$  is positive.

**Lemma 21.**  $\det(\mathbf{M}) > 0$  for every  $(\alpha, \beta) \in \mathcal{R}'_3$ ,  $(\gamma, \delta)$  in the interior of (20) and  $(\gamma, \delta)$  in (24).

*Proof.* Observe that

$$\begin{aligned} U_1 + 3U_2 &= (R_8 + 2R_9/3 - 6R_2) + (3R_4 - 2R_6) + (R_9/3 - 4R_7/3) \\ &\quad + (3R_5/2 - 2R_7/2) + (3R_5/2 - 6R_3) \\ &> 0, \end{aligned}$$

where the last inequality follows by Lemma 21. Once again by Lemma 21, we have  $U_1 > 0$  and hence  $U_2/U_1 > -1/3$ . Thus, (29) gives

$$\det(\mathbf{H}) > \frac{U_1}{D}(2R_1 + U_2) = \frac{U_1}{D}[R_4 + R_5 + 2(R_1 - R_2 - R_3)] > 0,$$

where the last inequality follows from Lemma 16 and Observation 14.  $\square$

*Proof of Lemma 11.* As in the proof of Lemma 10, Lemmata 18 and 21 yield that  $g_{\alpha,\beta}(\gamma, \delta, \varepsilon)$  achieves its unique maximum in the region (3) at the point  $(\gamma^*, \delta^*, \varepsilon^*)$ , for every  $(\alpha, \beta) \in \mathcal{R}'_3$ . We next show that  $g_{\alpha,\beta}(\gamma, \delta, \varepsilon) := \Phi_2(\alpha, \beta, \gamma, \delta, \varepsilon)$  also achieves its unique maximum in the region (3) at the point  $(\gamma^*, \delta^*, \varepsilon^*)$  in a small neighborhood of  $\mathcal{R}'_3$ .

First note that  $\Phi_2$  is continuous. By Lemma 12, we have for sufficiently small  $\chi > 0$ , the maximum of  $g_{\alpha,\beta}$  cannot be obtained on the boundary of the region (3).

Note that the derivatives of  $\Phi_2$  are continuous. It follows that for sufficiently small  $\chi > 0$ , all stationary points of  $g_{\alpha,\beta}$  have to be close to the point  $(\gamma^*, \delta^*, \varepsilon^*)$ . We can choose  $\chi$  such that  $\det(\mathbf{H}) > 0$  in the neighborhood of the point  $(\gamma^*, \delta^*, \varepsilon^*)$ , which implies that  $g_{\alpha,\beta}$  has a unique stationary point and it is a maximum.  $\square$

## 6 Remaining Proofs of Technical Lemmas

### 6.1 Proof of Lemma 13

We define  $W_3$  to be the numerator of  $W_{11}$  minus the denominator of  $W_{11}$ , and  $W_4$  to be the numerator of  $W_{21}$  minus the denominator of  $W_{21}$ ; more precisely

$$W_3 = (\alpha - \gamma - \hat{\varepsilon})\hat{\varepsilon}(1 - 2\alpha + \gamma) - \hat{\eta}(\alpha - \gamma)^2, \quad (30)$$

$$W_4 = (\beta - \delta - \hat{\eta})\hat{\eta}(1 - 2\beta + \delta) - \hat{\varepsilon}(\beta - \delta)^2. \quad (31)$$

Substituting the expression for  $\hat{\varepsilon}$  and simplifying we obtain

$$\begin{aligned} W_3 &:= ((\alpha + \beta - 1 + \sqrt{D})/2)\hat{\varepsilon}(1 - 2\alpha + \gamma) - \hat{\eta}(\alpha - \gamma)^2, \\ W_4 &:= ((\alpha + \beta - 1 + \sqrt{D})/2)\hat{\eta}(1 - 2\beta + \delta) - \hat{\varepsilon}(\beta - \delta)^2. \end{aligned}$$

By expanding  $W_3$  and  $W_4$ , we have

$$\begin{aligned} W_3 &= W_{31} + W_{32}\sqrt{D}, \\ W_4 &= W_{41} + W_{42}\sqrt{D}, \end{aligned}$$

where

$$\begin{aligned} W_{31} &= ((3/2)\beta - (1/2)\beta^2 - \delta - (3/2)\alpha\beta + \delta\alpha)\gamma \\ &\quad + \beta + (5/2)\beta\alpha^2 + (1/2)\alpha^3 + (3/2)\alpha - (3/2)\alpha^2 \\ &\quad - (1/2)\beta^2 - 1/2 + \delta\alpha - (7/2)\alpha\beta - \delta\alpha^2 + \beta^2\alpha, \\ W_{32} &= \alpha\beta - (1/2)\beta\gamma - \alpha - (1/2)\beta + (1/2)\alpha^2 + 1/2, \\ W_{41} &= ((3/2)\alpha - (1/2)\alpha^2 - \gamma - (3/2)\alpha\beta + \gamma\beta)\delta \\ &\quad + \alpha + (5/2)\alpha\beta^2 + (1/2)\beta^3 + (3/2)\beta - (3/2)\beta^2 \\ &\quad - (1/2)\alpha^2 - 1/2 + \gamma\beta - (7/2)\alpha\beta - \gamma\beta^2 + \alpha^2\beta, \\ W_{42} &= \alpha\beta - (1/2)\alpha\delta - \beta - (1/2)\alpha + (1/2)\beta^2 + 1/2. \end{aligned}$$

Note that for every  $(\alpha, \beta) \in \mathcal{R}$ ,  $W_{32} > 0$  when  $0 < \gamma < \alpha$ , and  $W_{42} > 0$  when  $0 < \delta < \beta$ . To see  $W_{32} > 0$  note that  $\alpha\beta - (1/2)\beta\gamma - \alpha - (1/2)\beta + (1/2)\alpha^2 + 1/2 \geq \alpha\beta - (1/2)\beta\alpha - \alpha - (1/2)\beta + (1/2)\alpha^2 + 1/2 = (1/2)(1 - \alpha)(1 - \alpha - \beta) > 0$ , since  $\alpha + \beta < 1$ ; inequality  $W_{42} > 0$  is the same (after renaming the variables).

Note that  $W_{31}$  is a linear function in  $\gamma$  and we have

$$\frac{dW_{31}}{d\gamma} = (3/2)\beta - (1/2)\beta^2 - \delta - (3/2)\alpha\beta + \delta\alpha,$$

which is positive for all  $(\alpha, \beta) \in \mathcal{R}$  and  $0 < \delta < \beta$ . To see this note

$$\begin{aligned} (3/2)\beta - (1/2)\beta^2 - \delta - (3/2)\alpha\beta + \delta\alpha &= (1 - \alpha)((3/2)\beta - \delta) - (1/2)\beta^2 \\ &\geq (1 - \alpha)(1/2)\beta - (1/2)\beta^2 = (1/2)\beta(1 - \alpha - \beta) > 0. \end{aligned}$$

Moreover, we have  $W_{31}$  is negative when  $\gamma = \alpha$ ,  $(\alpha, \beta) \in \mathcal{R}$  and  $0 < \delta < \beta$  (after substituting  $\gamma = \alpha$  into  $W_{31}$  we obtain  $-(1 - \alpha)(1 - \alpha - \beta)^2/2 < 0$ ). Hence,  $W_{31} < 0$  for all  $(\alpha, \beta) \in \mathcal{R}$ ,  $0 < \gamma < \alpha$  and  $0 < \delta < \beta$ .

By the same proof, we can show that  $W_{41} < 0$  for all  $(\alpha, \beta) \in \mathcal{R}$ ,  $0 < \gamma < \alpha$  and  $0 < \delta < \beta$  (note that  $W_{31}$  and  $W_{41}$  are the same after renaming the variables).

Let

$$\begin{aligned} W_5 &= (W_{31}/W_{32})^2 - D, \\ W_6 &= (W_{41}/W_{42})^2 - D. \end{aligned}$$

Note that the signs of  $W_3$  and  $W_5$  are opposite, and the signs of  $W_4$  and  $W_6$  are opposite.

After substituting  $W_{31}, W_{32}, W_{41}, W_{42}$  and simplifications, we obtain

$$\begin{aligned} W_5 &= -\frac{4(\beta - \delta)(\alpha - \gamma)^2((1 - \alpha)^2\delta + \beta^2(2\alpha - 1 - \gamma))}{(2\alpha\beta - \beta\gamma - 2\alpha - \beta + \alpha^2 + 1)^2}, \\ W_6 &= -\frac{4(\beta - \delta)^2(\alpha - \gamma)((1 - \beta)^2\gamma + \alpha^2(2\beta - 1 - \delta))}{(\beta^2 - \delta\alpha + 1 - 2\beta - \alpha + 2\alpha\beta)^2}. \end{aligned}$$

Hence,

$$W_{11} \geq 1 \iff W_5 \leq 0 \iff (1 - \alpha)^2\delta + \beta^2(2\alpha - 1 - \gamma) \geq 0,$$

and

$$W_{21} \geq 1 \iff W_6 \leq 0 \iff (1 - \beta)^2\gamma + \alpha^2(2\beta - 1 - \delta) \geq 0.$$

Finally, we analyze the conditions for  $W_{12} \geq 1$  and  $W_{22} \geq 1$ . It is straightforward to see that

$$W_{12} \geq 1 \iff (\alpha - \gamma)^2 \geq (1 - 2\alpha + \gamma)\gamma \iff \gamma \leq \alpha^2,$$

and

$$W_{22} \geq 1 \iff (\beta - \delta)^2 \geq (1 - 2\beta + \delta)\delta \iff \delta \leq \beta^2.$$

## 6.2 Proof of Lemma 16

We have

$$-R_1 + R_2 + R_3 = (\beta - \delta) \left( -\frac{1}{\alpha - \gamma - \hat{\varepsilon}} - \frac{1}{\hat{\eta}} + \frac{1}{\hat{\varepsilon}} \right) - \frac{\sqrt{D}}{\hat{\varepsilon}} + \frac{\sqrt{D}}{1 - 2\alpha + \gamma} + \frac{2\sqrt{D}}{\alpha - \gamma}.$$

Multiplying by the denominators we let

$$P_1 = (-R_1 + R_2 + R_3)\hat{\varepsilon}\hat{\eta}(1 - 2\alpha + \gamma)(\alpha - \gamma)(\alpha - \gamma - \hat{\varepsilon}) = P_{11} + P_{12}\sqrt{D},$$

where

$$\begin{aligned} P_{11} = & 1 - (1/2)\delta\alpha + 17\alpha\beta + (9/2)\delta\gamma - 5\beta\gamma + 21\alpha\gamma\beta\delta - (37/2)\alpha^2\gamma\beta\delta - 5\alpha\gamma\beta\delta^2 + (5/2)\alpha\gamma\beta^2\delta \\ & + 8\gamma^2\alpha\delta\beta - 5\alpha - 3\beta - \delta + 10\alpha^2 + 3\beta^2 + 3\delta\beta - 10\alpha^3 + 5\alpha^4 - \beta^3 + 15\alpha\gamma\beta - (13/2)\alpha\beta\delta \\ & - (27/2)\alpha\gamma\delta - (5/2)\beta\gamma\delta - 4\alpha^2\beta\delta + (27/2)\alpha^2\gamma\delta - 15\alpha^2\gamma\beta - 24\alpha\gamma\beta^2 - 8\gamma^2\beta\delta \\ & + (17/2)\alpha\beta^2\delta - (5/2)\beta^2\gamma\delta - 3\alpha\beta\delta^2 + 3\beta\gamma\delta^2 + (15/2)\alpha^3\beta\delta + 4\alpha^2\beta\delta^2 - (11/2)\alpha^2\beta^2\delta \\ & - (9/2)\alpha^3\gamma\delta + 3\alpha^2\gamma\delta^2 + 5\alpha^3\gamma\beta + 17\alpha^2\gamma\beta^2 + 4\alpha\gamma\beta^3 - 3\gamma^2\alpha\delta^2 - 5\gamma^2\alpha\beta^2 + \gamma^2\beta\delta^2 - 3\beta^2\delta \\ & + 3\delta^2\alpha - 3\delta^2\gamma - 3\alpha^2\delta^2 + (7/2)\alpha^4\delta - 8\alpha^4\beta - 15\alpha^3\beta^2 - 4\alpha^2\beta^3 + 3\gamma^2\delta^2 - \gamma^2\beta^3 - 33\alpha^2\beta \\ & + (15/2)\alpha^2\delta - 16\alpha\beta^2 + 7\beta^2\gamma - (19/2)\alpha^3\delta + 27\alpha^3\beta + 28\alpha^2\beta^2 + 5\gamma^2\beta^2 + 4\alpha\beta^3 - 2\beta^3\gamma \\ & + \delta\beta^3 - (3/2)\alpha\beta^3\delta + (1/2)\beta^3\gamma\delta - \alpha^5, \end{aligned}$$

and

$$\begin{aligned} P_{12} = & -1 - (1/2)\delta\alpha - 9\alpha\beta - (5/2)\delta\gamma + 3\beta\gamma - 2\alpha\gamma\beta\delta + 4\alpha + 2\beta + \delta - 6\alpha^2 - \beta^2 - 2\delta\beta \\ & + 4\alpha^3 - \alpha^4 - 6\alpha\gamma\beta + 4\alpha\beta\delta + 5\alpha\gamma\delta - \alpha^2\beta\delta - (5/2)\alpha^2\gamma\delta + 3\alpha^2\gamma\beta + 4\alpha\gamma\beta^2 + \gamma^2\beta\delta \\ & - (3/2)\alpha\beta^2\delta + (1/2)\beta^2\gamma\delta - \alpha\gamma\delta^2 + \beta^2\delta - \delta^2\alpha + \delta^2\gamma + \alpha^2\delta^2 + 12\alpha^2\beta - 2\alpha^2\delta + 4\alpha\beta^2 \\ & - 2\beta^2\gamma + (3/2)\alpha^3\delta - 5\alpha^3\beta - 4\alpha^2\beta^2 - \gamma^2\beta^2. \end{aligned}$$

The following claim is proved using the **Resolve** function of the Mathematica system in Appendix A.2.

**Claim 22.**  $P_{11} > 0$  and  $P_{12} < 0$  for all  $(\alpha, \beta) \in \mathcal{R}$  and  $(\gamma, \delta)$  in the interior of (20).

From Claim 22 we have that  $P_{11} - P_{12}\sqrt{D} > 0$  and hence showing  $P_{11} + P_{12}\sqrt{D} < 0$  is equivalent to showing  $P_{11}^2 - P_{12}^2 D < 0$  which in turn is equivalent to showing that  $P_2 := (P_{11}/P_{12})^2 - D$  is negative. We have

$$P_2 = (P_{11}/P_{12})^2 - D = -\frac{(\beta - \delta)^2(\alpha - \gamma)^3 P_{21}}{P_{12}^2},$$

where

$$\begin{aligned} P_{21} = & -8\delta\alpha + 20\alpha\gamma\beta\delta - 10\alpha^2\gamma\beta\delta + 2\alpha\gamma\beta\delta^2 + 12\alpha\gamma\beta^2\delta + 2\delta + 2\delta^2 - 8\delta\beta + 4\beta^3 + 34\alpha\beta\delta \\ & - 10\beta\gamma\delta - 44\alpha^2\beta\delta + 8\alpha\beta^2\delta - 4\beta^2\gamma\delta - 14\alpha\beta\delta^2 - 2\beta\gamma\delta^2 + 18\alpha^3\beta\delta + 6\alpha^2\beta\delta^2 - 10\alpha^2\beta^2\delta \\ & + 9\alpha^2\gamma\delta^2 - 16\alpha\gamma\beta^3 - 18\alpha\gamma\delta^2 - 2\beta^2\delta - 15\delta^2\alpha + 9\delta^2\gamma + 24\alpha^2\delta^2 + 2\alpha^4\delta + 16\alpha^2\beta^3 \\ & + 4\gamma^2\beta^3 + 12\alpha^2\delta - 8\alpha^3\delta - 16\alpha\beta^3 + 8\beta^3\gamma - 4\delta\beta^3 + 6\alpha\beta^3\delta - 2\beta^3\gamma\delta + 8\delta^2\beta + 2\beta^2\delta^2 \\ & + 8\delta^3\alpha - 4\delta^3\alpha^2 - 11\delta^2\alpha^3 - 3\delta^2\alpha\beta^2 + \delta^2\gamma\beta^2 - 4\delta\gamma^2\beta^2 - 4\delta^3. \end{aligned}$$

The following claim is proved using the **Resolve** function of the Mathematica system in Appendix A.3.

**Claim 23.**  $P_{21} > 0$  for all  $(\alpha, \beta) \in \mathcal{R}$  and  $(\gamma, \delta)$  in the interior of (20).

From Claim 23 we have that  $P_2 < 0$  which implies  $P_{11} + P_{12}\sqrt{D} < 0$  and this completes the proof of Lemma 16.

### 6.3 Proof of Lemma 18

We will use the following technical lemma in the proof of Lemma 18.

**Lemma 24.** *For every  $(\alpha, \beta) \in \mathcal{R}$ , and  $(\gamma, \delta)$  in the interior of (20), we have*

$$(-R_1 + R_2 + R_3)(-R_1 + R_6 + R_7) - R_1^2 < 0, \quad (32)$$

$$(-R_1 + R_2 + R_3)(-R_1 - R_8 - R_9) - R_1^2 \geq 0, \quad (33)$$

and

$$(-R_1 + R_6 + R_7)(-R_1 - R_4 - R_5) - R_1^2 \geq 0. \quad (34)$$

*Proof of Lemma 24.* We first prove inequality (32). We have that

$$(-R_1 + R_2 + R_3)(-R_1 + R_6 + R_7) = (R_1 - R_2 - R_3)(R_1 - R_6 - R_7) < R_1^2,$$

where the last inequality uses Lemma 16 and the positivity of the  $R_i$  (Observation 14). This establishes (32).

We next prove (33), noting that inequality (34) follows by an analogous argument. The left-hand side of (33) multiplied by the denominators and simplified is

$$\begin{aligned} P_5 &= ((-R_1 + R_2 + R_3)(-R_1 - R_8 - R_9) - R_1^2)\delta(\alpha - \gamma)\hat{\varepsilon}\hat{\eta}(1 - 2\alpha + \gamma)(\alpha - \gamma - \hat{\varepsilon})/\sqrt{D} \\ &= P_{51} + P_{52}\sqrt{D}, \end{aligned}$$

where

$$\begin{aligned} P_{51} &= -1 - 4\beta\gamma^2\delta\alpha + 3\delta\alpha - 17\alpha\beta - 3\delta\gamma + 5\beta\gamma - 14\alpha\beta\gamma\delta + 11\alpha^2\beta\gamma\delta + 5\alpha + 3\beta - 10\alpha^2 - 3\beta^2 \\ &\quad - 15\alpha\beta\gamma + 9\delta\alpha\gamma - 3\alpha\beta\delta + 10\alpha^2\beta\delta + 15\alpha^2\beta\gamma + 24\alpha\beta^2\gamma + 3\beta\gamma\delta + 4\beta\gamma^2\delta - 9\delta\alpha^2\gamma \\ &\quad - 7\alpha^3\beta\delta - 5\alpha^3\beta\gamma - 17\alpha^2\beta^2\gamma - 4\alpha\beta^3\gamma + 5\beta^2\gamma^2\alpha + 3\delta\alpha^3\gamma + 33\alpha^2\beta - 9\delta\alpha^2 + 16\alpha\beta^2 \\ &\quad - 27\alpha^3\beta - 28\alpha^2\beta^2 - 7\beta^2\gamma - 5\beta^2\gamma^2 + 9\delta\alpha^3 - 4\alpha\beta^3 + 8\alpha^4\beta + 15\alpha^3\beta^2 + 4\alpha^2\beta^3 + 2\beta^3\gamma \\ &\quad + \beta^3\gamma^2 - 3\delta\alpha^4 + 10\alpha^3 - 5\alpha^4 + \beta^3 + \alpha^5, \end{aligned}$$

and

$$\begin{aligned} P_{52} &= 1 - 2\delta\alpha\gamma + 6\alpha\beta\gamma - 3\alpha^2\beta\gamma - 4\alpha\beta^2\gamma + \delta\alpha^2\gamma - 4\alpha + 6\alpha^2 - 2\beta - 4\alpha^3 + \alpha^4 + \beta^2 + 9\alpha\beta \\ &\quad - 3\beta\gamma - \delta\alpha + \delta\gamma + 2\delta\alpha^2 - 12\alpha^2\beta - 4\alpha\beta^2 + 5\alpha^3\beta + 4\alpha^2\beta^2 + 2\beta^2\gamma + \beta^2\gamma^2 - \delta\alpha^3. \end{aligned}$$

The following claim is proved using the `Resolve` function of the Mathematica system in Appendix A.4.

**Claim 25.**  $P_{51} < 0$ ,  $P_{52} > 0$  for all  $(\alpha, \beta) \in \mathcal{R}$  and  $(\gamma, \delta)$  in the interior of (20).

From Claim 25 we have that  $P_{52}\sqrt{D} - P_{51} > 0$  and hence the sign of  $P_5 = P_{51} + P_{52}\sqrt{D}$  is the same as the sign of  $DP_{52}^2 - P_{51}^2$  which is the same as the sign of

$$D - (P_{51}/P_{52})^2 = \frac{4(\beta - \delta)(\alpha - \gamma)^3 \left( (1 - \alpha)^2\delta + \beta^2(2\alpha - 1 - \gamma) \right)^2}{P_{52}^2} > 0.$$

Hence  $P_5 > 0$  which implies (33).  $\square$

*Proof of Lemma 18.* From  $\alpha + \beta + \Delta(\Delta - 2)\alpha\beta \leq 1$  we have

$$(\Delta - 1)^2 \leq (1 - \alpha)(1 - \beta)/(\alpha\beta) =: R_{11}. \quad (35)$$

Lemma 24 implies that the coefficient of  $(\Delta - 1)$  in (28) is positive and the coefficient of  $(\Delta - 1)^2$  in (28) is negative. Hence, also using (35), we have

$$\begin{aligned} \det(M) &\geq \frac{1}{D} \left\{ R_{11} [(-R_1 + R_2 + R_3)(-R_1 + R_6 + R_7) - R_1^2] + \right. \\ &\quad \left. + [(-R_1 - R_8 - R_9)(-R_1 - R_4 - R_5) - R_1^2] \right\} \\ &> \frac{1}{D} \left( -R_1 R_2 R_{11} - R_1 R_6 R_{11} + R_1 R_4 + R_1 R_8 + \right. \\ &\quad \left. + R_5 R_9 + R_3 R_7 R_{11} + R_1 R_5 + R_1 R_9 - R_1 R_3 R_{11} - R_1 R_7 R_{11} + \right. \\ &\quad \left. + R_2 R_7 R_{11} + R_3 R_6 R_{11} \right). \end{aligned}$$

We will show

$$-R_1 R_2 R_{11} - R_1 R_6 R_{11} + R_1 R_4 + R_1 R_8 > 0, \quad (36)$$

and

$$R_5 R_9 + R_3 R_7 R_{11} + R_1 R_5 + R_1 R_9 - R_1 R_3 R_{11} - R_1 R_7 R_{11} + R_2 R_7 R_{11} + R_3 R_6 R_{11} > 0. \quad (37)$$

To prove (36), note that

$$\begin{aligned} &-R_1 R_2 R_{11} - R_1 R_6 R_{11} + R_1 R_4 + R_1 R_8 = \\ &\frac{\sqrt{D}(1 - \alpha - \beta)}{1 - \alpha - \beta - \hat{\varepsilon} - \hat{\eta}} \left( \frac{1}{\gamma} + \frac{1}{\delta} - \frac{(1 - \alpha)(1 - \beta)}{\alpha\beta(1 - 2\alpha + \gamma)} - \frac{(1 - \alpha)(1 - \beta)}{\alpha\beta(1 - 2\beta + \delta)} \right). \end{aligned}$$

The positivity of (36) follows from the following claim.

**Claim 26.**

$$\frac{1}{\gamma} + \frac{1}{\delta} - \frac{(1 - \alpha)(1 - \beta)}{\alpha\beta(1 - 2\alpha + \gamma)} - \frac{(1 - \alpha)(1 - \beta)}{\alpha\beta(1 - 2\beta + \delta)} > 0,$$

for every  $(\alpha, \beta) \in \mathcal{R}_3 \supset \mathcal{R}_\Delta$ ,  $(\gamma, \delta)$  in the interior of (20), and  $(\gamma, \delta)$  in (23).

*Proof of Claim 26.*

$$\begin{aligned} &\left( \frac{1}{\gamma} + \frac{1}{\delta} - \frac{(1 - \alpha)(1 - \beta)}{\alpha\beta(1 - 2\alpha + \gamma)} - \frac{(1 - \alpha)(1 - \beta)}{\alpha\beta(1 - 2\beta + \delta)} \right) \alpha\beta\gamma\delta(1 - 2\alpha + \gamma)(1 - 2\beta + \delta) \\ &= -2\gamma\delta + \delta\alpha\beta + \gamma\alpha\beta - 4\delta\alpha\beta\gamma - 2\delta\alpha\beta^2 + \delta^2\alpha\beta - 2\delta\alpha^2\beta + 4\delta\alpha^2\beta^2 - 2\delta^2\alpha^2\beta - 2\gamma\alpha\beta^2 \\ &\quad - 2\gamma\alpha^2\beta + 4\gamma\alpha^2\beta^2 + \gamma^2\alpha\beta - 2\gamma^2\alpha\beta^2 + 4\gamma\delta\beta - 2\gamma\delta\beta^2 + \gamma\delta^2\beta + 4\gamma\delta\alpha + \gamma\delta^2\alpha + \gamma^2\delta\beta \\ &\quad - 2\gamma\delta\alpha^2 + \gamma^2\delta\alpha - \gamma\delta^2 - \gamma^2\delta > 0, \end{aligned}$$

where the last inequality is proved using **Resolve** function of Mathematica system, see Appendix A.5.  $\square$



To show (37), we first note that

$$\begin{aligned}
& R_5 R_9 + R_3 R_7 R_{11} + R_1 R_5 + R_1 R_9 - R_1 R_3 R_{11} - R_1 R_7 R_{11} + R_2 R_7 R_{11} + R_3 R_6 R_{11} \\
&= \sqrt{D} \left( \frac{4(1-\beta-\gamma-\hat{\varepsilon})}{(\alpha-\gamma)} + \frac{(1-\alpha)(1-\beta)}{(1-2\alpha+\gamma)\alpha\beta} \frac{2(\alpha-\gamma-\hat{\varepsilon})}{\beta-\delta} + \frac{(1-\alpha)(1-\beta)}{(1-2\beta+\delta)\alpha\beta} \frac{2(\alpha-\gamma-\hat{\varepsilon})}{\alpha-\gamma} \right. \\
&\quad \left. - \frac{2(\alpha-\gamma-\hat{\varepsilon})^2}{(\alpha-\gamma)(\beta-\delta)} \left( \frac{1}{\hat{\eta}} + \frac{1}{\hat{\varepsilon}} \right) \left( \frac{(1-\alpha)(1-\beta)}{\alpha\beta} - \frac{1-\beta-\gamma-\hat{\varepsilon}}{\alpha-\gamma-\hat{\varepsilon}} \right) \right) \\
&> \frac{2\sqrt{D}(\alpha-\gamma-\hat{\varepsilon})}{\beta-\delta} \left( \frac{(1-\alpha)(1-\beta)}{(1-2\alpha+\gamma)\alpha\beta} - \frac{\alpha-\gamma-\hat{\varepsilon}}{(\alpha-\gamma)\hat{\eta}} \left( \frac{(1-\alpha)(1-\beta)}{\alpha\beta} - \frac{1-\beta-\gamma-\hat{\varepsilon}}{\alpha-\gamma-\hat{\varepsilon}} \right) \right) \\
&\quad + \frac{2\sqrt{D}(\alpha-\gamma-\hat{\varepsilon})}{\alpha-\gamma} \left( \frac{(1-\alpha)(1-\beta)}{(1-2\beta+\delta)\alpha\beta} - \frac{\alpha-\gamma-\hat{\varepsilon}}{(\beta-\delta)\hat{\varepsilon}} \left( \frac{(1-\alpha)(1-\beta)}{\alpha\beta} - \frac{1-\beta-\gamma-\hat{\varepsilon}}{\alpha-\gamma-\hat{\varepsilon}} \right) \right).
\end{aligned}$$

We will show

$$\frac{(1-\alpha)(1-\beta)}{(1-2\alpha+\gamma)\alpha\beta} - \frac{\alpha-\gamma-\hat{\varepsilon}}{(\alpha-\gamma)\hat{\eta}} \left( \frac{(1-\alpha)(1-\beta)}{\alpha\beta} - \frac{1-\beta-\gamma-\hat{\varepsilon}}{\alpha-\gamma-\hat{\varepsilon}} \right) > 0,$$

for every  $(\alpha, \beta) \in \mathcal{R}_3 \supset \mathcal{R}_\Delta$ ,  $(\gamma, \delta)$  in the interior of (20), and  $(\gamma, \delta)$  in (23). Then by symmetry, we have

$$\frac{(1-\alpha)(1-\beta)}{(1-2\beta+\delta)\alpha\beta} - \frac{\alpha-\gamma-\hat{\varepsilon}}{(\beta-\delta)\hat{\varepsilon}} \left( \frac{(1-\alpha)(1-\beta)}{\alpha\beta} - \frac{1-\beta-\gamma-\hat{\varepsilon}}{\alpha-\gamma-\hat{\varepsilon}} \right) > 0.$$

Let

$$\begin{aligned}
P_7 &= \left( \frac{(1-\alpha)(1-\beta)}{(1-2\alpha+\gamma)\alpha\beta} - \frac{\alpha-\gamma-\hat{\varepsilon}}{(\alpha-\gamma)\hat{\eta}} \left( \frac{(1-\alpha)(1-\beta)}{\alpha\beta} - \frac{1-\beta-\gamma-\hat{\varepsilon}}{\alpha-\gamma-\hat{\varepsilon}} \right) \right) \\
&\quad \alpha\beta\hat{\eta}(\alpha-\gamma)(1-2\alpha+\gamma) \\
&= P_{71} + P_{72}\sqrt{D},
\end{aligned}$$

where

$$\begin{aligned}
P_{71} &= (3/2)\alpha^2 + 4\alpha\beta + (1/2)\beta^2 - \alpha\delta - \gamma\beta + \gamma\delta + 1/2 - (3/2)\alpha - \beta + \delta\alpha\beta + (3/2)\gamma\alpha\beta \\
&\quad + \delta\alpha\beta\gamma - \delta\alpha^2\beta - (3/2)\gamma\alpha\beta^2 - (1/2)\gamma\alpha^2\beta - \gamma\delta\beta - \gamma\delta\alpha - (1/2)\alpha^3 - (9/2)\alpha^2\beta \\
&\quad - (5/2)\alpha\beta^2 + \gamma\beta^2 + \alpha^2\delta + (3/2)\alpha^3\beta + (5/2)\alpha^2\beta^2,
\end{aligned}$$

and

$$P_{72} = (1/2)\gamma\alpha\beta - 1/2 + (1/2)\beta + \alpha - (1/2)\alpha^2 - (1/2)\alpha\beta - (1/2)\alpha^2\beta.$$

The following claim is proved using the **Resolve** function of the Mathematica system in Appendix A.6.

**Claim 27.**  $P_{71} > 0$  and  $P_{72} < 0$  for every  $(\alpha, \beta) \in \mathcal{R}_3 \supset \mathcal{R}_\Delta$ ,  $(\gamma, \delta)$  in the interior of (20), and  $(\gamma, \delta)$  in (23).

From Claim 27 we have that the following expression has the same sign as  $P_7$ :

$$(P_{71}/P_{72})^2 - D = \frac{P_{71}^2 - P_{72}^2 D}{P_{72}^2},$$

where

$$P_{71}^2 - P_{72}^2 D > 0.$$

The last inequality is true for every every  $(\alpha, \beta) \in \mathcal{R}_3 \supset \mathcal{R}_\Delta$ ,  $(\gamma, \delta)$  in the interior of (20), and  $(\gamma, \delta)$  in (23); it is proved using the **Resolve** function of the Mathematica system, see Appendix A.7.  $\square$

## 6.4 Proof of Lemma 19

We first prove the following upper bound on  $(\Delta - 1)^2$ .

**Proposition 28.** *For every  $\Delta \geq 3$ ,  $(\alpha, \beta) \in \mathcal{R}_\Delta$ ,  $(\gamma, \delta)$  in the interior of (20), and  $(\gamma, \delta)$  in (24), we have*

$$(\Delta - 1)^2 \leq \frac{(1 - \alpha)(1 - \beta)}{\alpha\beta} < \frac{1 - \beta - \gamma - \hat{\varepsilon}}{\alpha - \gamma - \hat{\varepsilon}}$$

*Proof of Proposition 28.* The first inequality is straightforward from  $\alpha + \beta + \Delta(\Delta - 2)\alpha\beta \leq 1$ . We next prove that  $(1 - \alpha)(1 - \beta)(\alpha - \gamma - \hat{\varepsilon}) < \alpha\beta(1 - \beta - \gamma - \hat{\varepsilon})$ . We have

$$\begin{aligned} & \alpha\beta(1 - \beta - \gamma - \hat{\varepsilon}) - (1 - \alpha)(1 - \beta)(\alpha - \gamma - \hat{\varepsilon}) \\ &= \frac{1}{2}(1 - \alpha - \beta)(1 - \alpha - \beta + 2\alpha\beta - \sqrt{D}) > 0, \end{aligned}$$

where the last inequality follows from

$$D = (1 - \alpha - \beta)^2 + 4(\alpha - \gamma)(\beta - \delta) < (1 - \alpha - \beta + 2\alpha\beta)^2.$$

The last inequality is true when  $\gamma > \alpha^2$  and  $\delta > \beta^2$  (to see this note  $(1 - \alpha - \beta + 2\alpha\beta)^2 - (1 - \alpha - \beta)^2 = 4(\alpha - \alpha^2)(\beta - \beta^2) > 4(\alpha - \gamma)(\beta - \delta)$ ).  $\square$

Let  $R_{10} = (1 - \beta - \gamma - \hat{\varepsilon})/(\alpha - \gamma - \hat{\varepsilon})$ . Note that  $R_7 R_{10} = R_9$ ,  $R_3 R_{10} = R_5$ .

Lemma 24 implies that the coefficient of  $(\Delta - 1)$  in (28) is positive and the coefficient of  $(\Delta - 1)^2$  in (28) is negative. Hence, also using Proposition 28, we have

$$\begin{aligned} \det(M) &\geq \frac{1}{D} (R_{10} ((-R_1 + R_2 + R_3)(-R_1 + R_6 + R_7) - R_1^2) \\ &\quad + ((-R_1 - R_8 - R_9)(-R_1 - R_4 - R_5) - R_1^2)), \\ &> \frac{1}{D} (-R_1 R_2 R_{10} - R_1 R_6 R_{10} + R_1 R_4 + R_1 R_8 + R_5 R_9 + R_3 R_7 R_{10} + R_2 R_9 + R_5 R_6). \end{aligned}$$

We will prove that for every  $(\alpha, \beta) \in \mathcal{R}_3 \supset \mathcal{R}_\Delta$ ,  $\alpha, \beta \leq 1/2$ ,  $(\gamma, \delta)$  in the interior of (20), and  $(\gamma, \delta)$  in (24),

$$R_1 R_4 - R_1 R_2 R_{10} + \frac{1}{2}(R_5 R_9 + R_3 R_7 R_{10}) + R_2 R_9 > 0, \quad (38)$$

and then by symmetry, we also have

$$R_1 R_8 - R_1 R_6 R_{10} + \frac{1}{2}(R_5 R_9 + R_3 R_7 R_{10}) + R_5 R_6 > 0.$$

The left-hand side of (38) can be written as the sum of the following two terms:

$$\frac{(1 - \alpha - \beta)\sqrt{D}}{1 - \alpha - \beta - \hat{\varepsilon} - \hat{\eta}} \left( \frac{1}{\gamma} - \frac{1}{1 - 2\alpha + \gamma} \right), \quad (39)$$

and

$$\frac{\sqrt{D}}{(1 - 2\alpha + \gamma)\hat{\eta}} \left( \frac{2(1 - \alpha)(1 - \alpha - \beta - \hat{\varepsilon})}{\alpha - \gamma} - \frac{(1 - \alpha - \beta)^2}{\hat{\varepsilon}} \right). \quad (40)$$

We have (39) is non-negative, since  $1 - 2\alpha \geq 0$ .

For (40), we only need to prove

$$\frac{1 - \alpha - \beta - \hat{\varepsilon}}{\alpha - \gamma} > \frac{(1 - \alpha - \beta)^2}{\hat{\varepsilon}},$$

since  $1 - 2\alpha \geq 0$ . By (19), it is equivalent to prove

$$1 - \alpha - \beta - \hat{\varepsilon} - \hat{\eta} - (1 - \alpha - \beta)^2 > 0. \quad (41)$$

To prove (41), we have

$$1 - \alpha - \beta - \hat{\varepsilon} - \hat{\eta} - (1 - \alpha - \beta)^2 = -(1 - \alpha - \beta)^2 - \alpha - \beta + \gamma + \delta + \sqrt{D},$$

and

$$\begin{aligned} D - (-(1 - \alpha - \beta)^2 - \alpha - \beta + \gamma + \delta)^2 &= 2\gamma + 2\delta - 2\alpha^2 - 2\beta^2 - 6\alpha\delta - 6\gamma\beta + 2\gamma\delta - 2\beta\delta - \delta^2 \\ &\quad + 6\alpha\beta^2 + 6\alpha^2\beta - 6\alpha^2\beta^2 - 2\alpha\gamma - 4\alpha^3\beta + 2\alpha^2\gamma + 2\alpha^2\delta \\ &\quad - 4\alpha\beta^3 + 2\beta^2\gamma + 2\beta^2\delta - \gamma^2 + 4\alpha\beta\delta + 4\alpha\beta\gamma + 2\alpha^3 \\ &\quad + 2\beta^3 - \alpha^4 - \beta^4. \end{aligned}$$

The following claim is proved using the **Resolve** function of the Mathematica system in Appendix A.8.

**Claim 29.**

$$D - (-(1 - \alpha - \beta)^2 - \alpha - \beta + \gamma + \delta)^2 > 0$$

for every  $(\alpha, \beta) \in \mathcal{R}$ ,  $\alpha \leq 1/2$ ,  $\beta \leq 1/2$ ,  $(\gamma, \delta)$  in the interior of (20), and  $(\gamma, \delta)$  in (24).

Since  $-(1 - \alpha - \beta)^2 - \alpha - \beta + \gamma + \delta < 0$ , we can conclude that (41) is true. Hence, we complete the proof of Lemma 19.

## 6.5 Proof of Lemma 20

We have

$$R_4 - R_6 = \sqrt{D} \cdot \frac{1 - 2\beta + \delta - \gamma}{\gamma(1 - 2\beta + \delta)} > 0,$$

where the inequality follows from (20).

We have

$$R_5 - R_7 = \frac{(1 - \alpha - \beta)(\alpha + \beta - \gamma - \delta) + (\beta - \delta - \alpha + \gamma)\sqrt{D}}{(\alpha - \gamma)(\beta - \delta)}.$$

If  $\beta - \delta - \alpha + \gamma \geq 0$ , then  $R_5 > R_7$ . We may assume that  $\beta - \delta - \alpha + \gamma < 0$ . To show  $R_5 > R_7$ , it is equivalent to prove that

$$(1 - \alpha - \beta)(\alpha + \beta - \gamma - \delta) > (\alpha - \gamma - \beta + \delta)\sqrt{D}.$$

We have

$$\frac{(1 - \alpha - \beta)^2(\alpha + \beta - \gamma - \delta)^2}{(\alpha - \gamma - \beta + \delta)^2} - D = \frac{4(\alpha - \gamma)(\beta - \delta)(1 - 2\beta - \gamma + \delta)(1 - 2\alpha - \delta + \gamma)}{(\alpha - \gamma - \beta + \delta)^2} > 0,$$

where the inequality follows from (20).

To show that  $R_5 > 4R_3$  and  $R_9 > 4R_7$ , it is sufficient to prove that  $1 - \beta - \gamma - \hat{\varepsilon} > 4(\alpha - \gamma - \hat{\varepsilon})$ , which follows from Proposition 28.

We next prove  $U_1 > 0$ . We first prove that  $R_8 > 2R_6$ . We have

$$R_8 - 2R_6 = \sqrt{D} \cdot \frac{1 - 2\beta - \delta}{\delta(1 - 2\beta + \delta)} \geq \sqrt{D} \cdot \frac{1 - 3\beta}{\delta(1 - 2\beta + \delta)} > 0,$$

where the first inequality follows from (20) and the last inequality follows from the fact that  $\beta \leq (3 - \sqrt{5})/4$ . Hence  $U_1 = R_8 - 2R_6 + R_9 - 2R_7 > 0$ .

We next show:

$$\frac{3R_8}{2} + R_9 > 9R_2.$$

by the fact that  $\hat{\varepsilon} := \frac{1}{2}(1 + \alpha - \beta - 2\gamma - \sqrt{D})$  and  $(1 - \alpha - \beta)^2 = \alpha\beta$ , the goal is then to show,

$$\frac{3\sqrt{D}}{2\delta} + \frac{\sqrt{\alpha\beta} + \sqrt{D}}{\beta - \delta} > \frac{9\sqrt{D}}{1 - 2\alpha + \gamma},$$

i.e.,

$$\frac{\sqrt{\alpha\beta}}{\sqrt{\alpha\beta + 4(\alpha - \gamma)(\beta - \delta)}} > \frac{9(\beta - \delta)}{1 - 2\alpha + \gamma} - \frac{3\beta}{2\delta} + 1/2.$$

Since the above inequality is monotone with respect to  $\gamma$ , so let  $\gamma = \gamma_{\min} = \frac{\alpha^2(1+\delta-2\beta)}{(1-\beta)^2}$ , and the goal is to show:

$$\frac{\sqrt{\alpha\beta}}{\sqrt{\alpha\beta + 4(\alpha - \gamma_{\min})(\beta - \delta)}} > \frac{9(\beta - \delta)}{1 - 2\alpha + \gamma_{\min}} - \frac{3\beta}{2\delta} + 1/2,$$

or equivalently,

$$\frac{1}{\sqrt{1 + 4(1 - \gamma_{\min}/\alpha)(1 - \delta/\beta)}} > \frac{9(\beta - \delta)}{1 - 2\alpha + \gamma_{\min}} - \frac{3\beta}{2\delta} + 1/2.$$

Replacing the term  $\gamma_{\min}$  in the left-hand side, we get,

$$\frac{1}{\sqrt{1 + 4(1 - \frac{\alpha(1+\delta-2\beta)}{(1-\beta)^2})(1 - \delta/\beta)}} > \frac{9(\beta - \delta)}{1 - 2\alpha + \gamma_{\min}} - \frac{3\beta}{2\delta} + 1/2.$$

Since  $\alpha > 1/2$  and  $\delta > \beta^2$ , replace them on the LHS, then our goal can be reduced to

$$\frac{1}{\sqrt{3 - 2\delta/\beta}} > \frac{9(\beta - \delta)}{1 - 2\alpha + \gamma_{\min}} - \frac{3\beta}{2\delta} + 1/2.$$

Let  $X = 1 - 2\alpha + \gamma_{\min} = \frac{(1-2\alpha)(1-\beta)^2 + \alpha^2(1-2\beta+\delta)}{(1-\beta)^2}$  and  $A = \frac{3\beta-2\delta}{\beta}$ . So we are going to show

$$2\delta X > \sqrt{A}(18\delta(\beta - \delta) - 3\beta X + \delta X),$$

i.e.,

$$4\delta^2 X^2 > A(18\delta(\beta - \delta) - 3\beta X + \delta X)^2,$$

when  $18\delta(\beta - \delta) - 3\beta X + \delta X > 0$ . The rest of the proof can be checked by using Mathematica since they are all polynomial constraints, see Appendix A.9.

## References

- [1] J. van den Berg and J. E. Steif. Percolation and the hard-core lattice gas model. *Stochastic Processes and their Applications*, 49(2):179–197, 1994.
- [2] M. Dyer, A. M. Frieze, and M. Jerrum. On counting independent sets in sparse graphs. *SIAM J. Comput.*, 31(5):1527–1541, 2002.
- [3] D. S. Gaunt and M. E. Fisher. Hard-Sphere Lattice Gases. I. Plane-Square Lattice. *Journal of Chemical Physics*, 43(8):2840–2863, 1965.
- [4] C. Greenhill. The complexity of counting colourings and independent sets in sparse graphs and hypergraphs. *Computational Complexity*, 9(1):52–72, 2000.
- [5] S. Janson, T. Łuczak, and A. Ruciński. *Random Graphs*. Wiley-Interscience, New York, 2000.
- [6] M. R. Jerrum, L. G. Valiant, and V. V. Vazirani. Random generation of combinatorial structures from a uniform distribution. *Theoretical Computer Science*, 43(2-3):169–186, 1986.
- [7] F. P. Kelly. Loss Networks. *Annals of Applied Probability*, 1(3):319–378, 1991.
- [8] D. A. Levin, Y. Peres, and E. L. Wilmer. *Markov Chains and Mixing Times*. American Mathematical Society, Providence, RI, 2009.
- [9] M. Molloy, H. Robalewska, R. W. Robinson, and N. C. Wormald. 1-factorizations of random regular graphs. *Random Structures and Algorithms*, 10(3):305–321, 1997.
- [10] E. Mossel, D. Weitz, and N. Wormald. On the hardness of sampling independent sets beyond the tree threshold. *Probability Theory and Related Fields*, 143(3-4):401–439, 2009.
- [11] A. Sly. Computational Transition at the Uniqueness Threshold. In *Proceedings of the 51st Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, 287–296, 2010. Full version available from the arXiv at: <http://arxiv.org/abs/1005.5584>
- [12] D. Štefankovič, S. Vempala, and E. Vigoda. Adaptive Simulated Annealing: A Near-optimal Connection between Sampling and Counting. *Journal of the ACM*, 56(3):1–36, 2009.
- [13] A. W. Strzebonski. Cylindrical algebraic decomposition using validated numerics. *J. Symb. Comput.*, 41(9):1021–1038, 2006.
- [14] A. Tarski. *A Decision Method for Elementary Algebra and Geometry*. RAND Corporation, Santa Monica, Calif., 1948.
- [15] L. G. Valiant. The Complexity of Enumeration and Reliability Problems. *SIAM J. Computing*, 8(3):410–421, 1979.
- [16] D. Weitz. Counting independent sets up to the tree threshold. In *Proceedings of the 38th Annual ACM Symposium on Theory of Computing (STOC)*, 140–149, 2006.
- [17] N.C. Wormald. Models of random regular graphs. In *Surveys in Combinatorics, 1999 (Canterbury)*, J.D. Lamb and D.A. Preece (eds), pp. 239–298. Cambridge University Press, Cambridge, 1999.

## A Mathematica Code

```
Clear["Global`*"]

SetSystemOptions["InequalitySolvingOptions" -> "CAD" -> True];
SetSystemOptions["InequalitySolvingOptions" -> "QuadraticQE" -> False];
SetSystemOptions["InequalitySolvingOptions" -> "LinearQE" -> False];

RR = alpha > 0 && beta > 0 && alpha + beta < 1;
RR3 = alpha > 0 && beta > 0 && alpha + beta + 3*alpha*beta < 1;
Inter22 = gamma > 0 && gamma < alpha && delta > 0 && delta < beta &&
    1 - 2*beta + delta - gamma > 0 && 1 - 2*alpha + gamma - delta > 0;
l25 = gamma > 0 && gamma < alpha^2 && delta > 0 &&
    delta < beta^2 && (1 - alpha)^2*delta + beta^2*(2*alpha - 1 - gamma) < 0 &&
    (1 - beta)^2*gamma + alpha^2*(2*beta - 1 - delta) < 0;
u26 = gamma > alpha^2 && gamma < alpha && delta > beta^2 &&
    delta < beta && (1 - alpha)^2*delta + beta^2*(2*alpha - 1 - gamma) > 0 &&
    (1 - beta)^2*gamma + alpha^2*(2*beta - 1 - delta) > 0;

DD = (1 - alpha - beta)^2 + 4*(alpha - gamma)*(beta - delta);

epsilon = 1/2*(1 + alpha - beta - 2*gamma - SQ);
eta = 1/2*(1 + beta - alpha - 2*delta - SQ);

W11 = (alpha - gamma - epsilon)* epsilon*(1 - 2*alpha + gamma)/(eta*(alpha - gamma)^2);
W12 = (alpha - gamma)^2/((1 - 2*alpha + gamma)*gamma);
W21 = (beta - delta - eta)*eta*(1 - 2*beta + delta)/(epsilon*(beta - delta)^2);
W22 = (beta - delta)^2/((1 - 2*beta + delta)*delta);

R1 = (1 - alpha - beta)/(1 - alpha - beta - epsilon - eta);
R2 = SQ/(1 - 2*alpha + gamma);
R3 = 2*(alpha - gamma - epsilon)/(alpha - gamma);
R4 = SQ/gamma;
R5 = 2*(1 - beta - gamma - epsilon)/(alpha - gamma);
R6 = SQ/(1 - 2*beta + delta);
R7 = 2*(alpha - gamma - epsilon)/(beta - delta);
R8 = SQ/delta;
R9 = 2*(1 - beta - gamma - epsilon)/(beta - delta);
R10 = (1 - beta - gamma - epsilon)/(alpha - gamma - epsilon);
R11 = (1 - alpha)*(1 - beta)/(alpha*beta);
```

### A.1 Mathematica Code for Proving Lemma 13

```
W3 = Expand[Expand[Numerator[W11]/2 - Denominator[W11]/2] /. {SQ^2 -> DD}];
Exponent[W3, SQ]
W31 = Coefficient[W3, SQ, 0]
W32 = Coefficient[W3, SQ, 1]
Resolve[Exists[{alpha, beta, gamma}, RR && Inter22 && W32 <= 0], Reals]

W4 = Expand[Expand[Numerator[W21]/2 - Denominator[W21]/2] /. {SQ^2 -> DD}];
Exponent[W4, SQ]
W41 = Coefficient[W4, SQ, 0]
W42 = Coefficient[W4, SQ, 1]
Resolve[Exists[{alpha, beta, delta}, RR && Inter22 && W42 <= 0], Reals]

W5 = FullSimplify[(W31/W32)^2 - DD]
W6 = FullSimplify[(W41/W42)^2 - DD]
```

### A.2 Mathematica Code for Proving Claim 22

```
FullSimplify[((-R1 + R2 + R3) - ((beta - delta)*(-1/(alpha - gamma - epsilon)
- 1/eta + 1/epsilon) - SQ/epsilon + SQ/(1 - 2*alpha + gamma) +
2*SQ/(alpha - gamma)))] /. {SQ -> Sqrt[DD]]}
P1 = Expand[FullSimplify[ExpandAll[((beta - delta)*(-1/(alpha - gamma - epsilon)
- 1/eta + 1/epsilon) - SQ/epsilon + SQ/(1 - 2*alpha + gamma) +
2*SQ/(alpha - gamma))*epsilon*eta*(1 - 2*alpha + gamma)*(alpha - gamma)*
(alpha - gamma - epsilon)]] /. {SQ^2 -> DD, SQ^3 -> SQ*DD, SQ^4 -> DD^2}];
Exponent[P1, SQ]
P11 = Coefficient[P1, SQ, 0]
Resolve[Exists[{alpha, beta, gamma, delta}, RR && Inter22 && P11 <= 0], Reals]
P12 = Coefficient[P1, SQ, 1]
Resolve[Exists[{alpha, beta, gamma, delta}, RR && Inter22 && P12 >= 0], Reals]
```

### A.3 Mathematica Code for Proving Claim 23

```
P2 = FullSimplify[(P11/P12)^2 - DD];
P21 = -FullSimplify[Numerator[P2]/((beta - delta)^2*(alpha - gamma)^3)]
Resolve[Exists[{alpha, beta, gamma, delta}, RR && Inter22 && P21 <= 0], Reals]
```

### A.4 Mathematica Code for Proving Claim 25

```
P5=Expand[FullSimplify[
  Expand[((-R1 + R2 + R3)*(-R1 - R8 - R9) - R1^2)*delta*(alpha - gamma)*
  epsilon* eta*(1 - 2*alpha + gamma)*(alpha - gamma - epsilon)/ SQ]/.
  {SQ -> Sqrt[DD]]}]/.{Sqrt[alpha^2 + (-1 + beta)^2 +
  alpha (-2 + 6 beta - 4 delta) + 4 (-beta + delta) gamma]->SQ}
Exponent[P5, SQ]
P51 = Coefficient[P5, SQ, 0]
Resolve[Exists[{alpha, beta, gamma, delta}, RR && Inter22 && P51 >= 0]]
P52 = Coefficient[P5, SQ, 1]
```



```
Resolve[Exists[{alpha, beta, gamma, delta}, RR && Inter22 && P52 <= 0]]
FullSimplify[DD - (P51/P52)^2]
```

### A.5 Mathematica Code for Proving Claim 26

```
Resolve[Exists[{alpha, beta, gamma, delta},
  FullSimplify[
    Expand[(-R2*R11 - R6*R11 + R4 + R8)/SQ*alpha*beta*gamma*
      delta*(1 - 2*alpha + gamma)*(1 - 2*beta + delta)]] <= 0
    && RR3 && l25], Reals]
```

### A.6 Mathematica Code for Proving Claim 27

```
P7 = FullSimplify[((1 - alpha)*(1 - beta)/((1 - 2*alpha + gamma)*alpha*beta) -
  (alpha - gamma - epsilon)/((alpha - gamma)*eta)*((1 - alpha)*
  (1 - beta)/(alpha*beta) - (1 - beta - gamma - epsilon)
  /(alpha - gamma - epsilon)))*alpha*beta*eta*(alpha - gamma)*
  (1 - 2*alpha + gamma)]
Exponent[P7, SQ]
P71 = Coefficient[P7, SQ, 0]
Resolve[Exists[{alpha, beta, gamma, delta}, RR3 && Inter22 && P71 <= 0], Reals]
P72 = Coefficient[P7, SQ, 1]
Resolve[Exists[{alpha, beta, gamma, delta}, RR3 && Inter22 && P72 >= 0], Reals]
```

### A.7 Mathematica Code for Proving Lemma 18

```
TP1 = Expand[P71^2 - P72^2*DD]
Resolve[Exists[{alpha, beta, gamma, delta}, RR3 && l25 && TP1 <= 0], Reals]
```

### A.8 Mathematica Code for Proving Claim 29

```
TP2 = Expand[DD - (-(1 - alpha - beta)^2 - alpha - beta + gamma + delta)^2]
Resolve[Exists[{alpha, beta, gamma, delta}, RR && alpha <= 1/2 && beta <= 1/2
  && u26 && TP2 <= 0], Reals]
```

### A.9 Mathematica Code for Proving Lemma 20

```
X = ((1 - 2*alpha)*(1 - beta)^2 + alpha^2*(1 - 2*beta + delta))/(1 - beta)^2;
A = (2*beta - 2*delta)/beta;
Resolve[Exists[{alpha, beta, gamma, delta},
  (1 - alpha - beta)^2 == alpha*beta && alpha > 1/2 &&
  alpha < 1 && beta > 0 && beta < 1 && Inter22 && u26 &&
  4*delta^2*X^2 <= A*(18*delta*(beta - delta) - 3*beta*X + delta*X)^2 &&
  18*delta*(beta - delta) - 3*beta*X + delta*X > 0], Reals]
```